Sähkötekniikan korkeakoulu
Tietoliikennetekniikan tutkinto-ohjelma

Jon Silander

Katsaus identiteetinhallinnan teknologioihin ja niiden tulevaisuuden näkymiin

Diplomityö, joka on jätetty opinnäytteenä tarkastettavaksi diplomi-insinöörin tutkintoa varten Espoossa 20.4.2013.

Valvoja **Professori Jukka Manner**

Ohjaaja **Antti Ropponen, FM (tietojenkäsittelytiede)**

AALTO-YLIOPISTO
SÄHKÖTEKNIIKAN KORKEAKOULU

DIPLOMITYÖN
TIIVISTELMÄ

Tekijä: Jon Silander

Työn nimi: Katsaus identiteetinhallinnan teknologioihin ja niiden tulevaisuuden näkymiin

Päivämäärä: 20.4.2013 Kieli: Suomi Sivumäärä: 6+84=90

Tietoliikenne ja tietoverkkotekniikan laitos

Professuuri: Tietoverkkotekniikka Koodi: S-38

Valvoja: Prof. Jukka Manner

Ohjaaja: FM Antti Ropponen

Digitaalisten identiteettien hallinta on nykypäivän organisaatioiden toiminnan kannalta lähes välttämättömyys ja identiteettien sekä niihin sidottujen oikeuksien ja valtuuksien määrän kasvaessa tarvitaan tähän tehtävään automatisoituja identiteetinhallintajärjestelmiä. Tällä hetkellä näiden järjestelmien ja -teknologioiden tarjonta on kuitenkin varsin hajanainen ja laaja, eikä siitä ole helppo muodostaa yhtenäistä kokonaiskuvaa ilman syvällistä perehtymistä alan kirjallisuuteen.

Tässä diplomityössä esitellään tiivistetysti keskeisimmät identiteetin- ja pääsynhallinnassa käytettävät käsitteet ja toiminnallisuudet sekä niihin soveltuvat protokollat ja standardit. Lisäksi työssä kuvataan identiteetinhallintajärjestelmän yleistetty arkkitehtuuri ja vertaillaan keskenään muutamia tunnettuja identiteetinhallintatuotteita. Teoriaosuuden loppuosassa esitellään vielä lyhyesti pilviteknologiaa ja arvioidaan sen vaikutusta identiteetinhallintajärjestelmiin. Arvioinnissa tarkasteltiin sekä hyötyjä että haittoja erilaisista toteutusnäkökulmista.

Työn tutkimusosuus koostuu asiantuntijakyselytutkimuksesta, jossa selvitettiin asiantuntijoiden näkökulmaa identiteetinhallintateknologian nykytilaan ja sen tulevaisuuden näkymiin. Kyselyn tuloksien pohjalta saatiin kartoitettua muutamia tilastollisesti merkittäviä heikkouksia ja vahvuuksia nykyteknologiassa. Heikkoudet keskittyivät nykyisten järjestelmien yleisen monimutkaisuuden sekä niiden hankalan toteuttamisen ja käytön ympärille siinä missä vahvuudet olivat yksittäisempiä aiheita kuten hakemistopalvelut. Tuloksista saatiin myös kuvaa identiteetin- ja pääsynhallintateknologioihin tulevaisuudessa vaikuttavien trendien, kuten pilvipalvelujen ja mobiililaitteiden, merkityksellisyyksistä.

Avainsanat: identiteetinhallinta, pääsynhallinta, digitaalinen, identiteetti, pilvi, pilvipalvelu, IAM, IdM

AALTO UNIVERSITY
SCHOOL OF ELECTRICAL ENGINEERING

ABSTRACT OF
MASTER'S THESIS

Author: Jon Silander

Title of thesis: A State of the Art Review of Identity Management Technologies and Their Future Trends

Date: 20.4.2013 Language: Finnish Number of pages: 6+84=90

Department of Communications and Netv

Professorship: Networking Technology Code of Professorship: S-38

Thesis supervisor: Prof. Jukka Manner

Thesis instructor: M.Sc. Antti Ropponen

Managing digital identities is almost a necessity for modern organizations and as the number of both identities and the rights and authorizations attached to them grows an automatic identity management system is needed to perform the task. Currently the variety of these systems and technologies, however, is vast, so it is difficult to form a complete view of the field without extensive research into the literature on the topic.

This thesis work showcases the most central terminology and functionalities of identity and access management, as wells the protocols and standards used. The work also presents a generic architecture for an identity management system and provides comparisons between a few of the widely known identity management products. In the final parts of the theory section there is a short introduction to cloud technology and an evaluation of its impact on identity management. The evaluation was carried out by examining the advantages and disadvantages from several implementation perspectives.

The research part of the work consists of an online survey aimed at identity and access management experts to provide an expert view on the current state and future trends of identity and access management. The results allowed the identification of a few statistically significant weaknesses and strengths of the current identity management technology. The weaknesses were heavily centered on the general complexity and difficulty of both use and implementation of current systems while the strengths were narrower topics like directory services. The results also provided an insight into the relevance of future trends that are likely to shape identity and access management technology such as cloud computing and mobile devices.

Keywords: identity management, access management, digital identity, cloud, IdM, IAM

Alkusanat

Tämän diplomityön synty ei ollut kivetön polku ja haluankin jakaa kiitosta kaikille niille, jotka olivat apuna ja tukena tämän pitkän ja raskaan polun varrella.

Tahdon kiittää työni valvojaa professori Jukka Mannerta rakentavasta ja rohkaisevasta ohjauksesta kaikkine hyvine neuvoineen niin itse työstä kuin sen kanssa selviämisestäkin.

Lisäksi haluan kiittää ohjaajaani Antti Ropposta ja kollegaani Hannu Koutaniemeä avusta aihealueen löytämisessä ja tuesta siihen liittyvissä kysymyksissä.

Viimeisenä, muttei vähäisimpänä, osoitan kiitokseni hyvälle ystävälleni Jyri Soppelalle vertaistuesta ja diplomityön vaikeiden hetkien kanssa sekä rakkaalle avopuolisolleni Kristiina Luomalalle kokonaisvaltaisesta tuesta koko koitoksen ajalta.

Helsingissä 13. päivänä huhtikuuta 2013

Jon Silander

Sisällysluettelo

1 Johdanto

Identiteettejä tarvitaan ihmisten välisessä arkisessa kanssakäymisessä määrittämään, kuka kukin on ja mitä ominaisuuksia ja oikeuksia heillä on. Yksilötasolla omien tuttavien, ystävien, perheenjäsenten sekä muun oman sosiaalisen piirin identiteettien hallinnointi sujuu intuitiivisesti ja yleensä vaivatta, koska käsiteltävien identiteettien määrä on pieni ja niille myönnetyt oikeudet vain abstraktisti määriteltyjä – kavereita voidaan pyytää kylään, mutta lähimmät ystävät voivat tulla kylään ilmoittamattakin ja niin edelleen. Nykyinen digitaalisten verkkojen aikakausi on monimutkaistanut tätä yksilötasollakin, koska henkilöillä on yhä useampia digitaalisia identiteettejä ja niiden oikeuksia joudutaan määrittämään aiempaa paljon tarkemmin. Organisaatiotasolla hallittavien identiteettien määrä kuitenkin nousee jo niin korkeaksi, että niiden hallinta ei ole enää yksinkertaista tai helppoa, koska organisaatiossa voi olla tuhansia tai jopa miljoonia henkilöitä, joilla kaikilla voi olla useampia identiteettejä. Tällaisten identiteettimäärien ja niiden oikeuksien hallinta manuaalisesti, jopa nykyisten digitaalisten järjestelmien aikana, on huomattavan raskasta, kuluttaa paljon ihmistyötunteja ja johtaa väistämättä manuaalisiin virheisiin.

Identiteetinhallintajärjestelmät pyrkivät tuomaan helpotusta tähän pääasiassa organisaatioiden ongelmaan automatisoimalla ja keskittämällä identiteettien hallintaa mahdollisimman pitkälle. Ne saavat identiteettitietonsa suoraan henkilöstöresurssien tietokannoista ja voivat täyttää tietoja ja myöntää oikeuksia automaattisesti perustuen henkilön asemaan ja rooliin organisaatiossa. Lisäksi järjestelmissä on usein sisäistä logiikkaa, joka mahdollistaa myös automaattisen identiteettipolitiikkojen kuten ”tehtävien eriyttämisen”, valvomisen tai henkilön käyttäjätilien ja kulkukortin sulkemisen työsuhteen päättyessä. Tämä vähentää inhimillisen erehdyksen tai virheen tuomaa riskiä organisaatiolle. Identiteetinhallintajärjestelmä myös välittää luomiensa identiteettien tiedot tarvittaessa edelleen muille sen piiriin kytketyille kohdejärjestelmille, joten identiteettejä tarvitsee hallinnoida vain yhdessä järjestelmässä usean sijasta. Keskitetty hallinta sekä automatisoinnin tuomien työaikasäästöjen ja manuaalisten virheiden vähentäminen ovatkin identiteetinhallintajärjestelmien pääasialliset hyödyt.

Tämä diplomityö on katsaus nykyisiin identiteetinhallintajärjestelmiin, jonka korkean tason termin alle sisältyvät myös pääsynhallintajärjestelmät identiteetinhallinnan kannalta keskeisiltä osin. Työn tarkoitus on luoda yhtenäinen kuva nykyisestä identiteetinhallintateknologiasta, vertailla ja arvioida markkinoilla olevia identiteetinhallintatuotteita sekä kartoittaa tulevaisuuden suuntauksien vaikutuksia identiteetinhallintaan. Nykytilan arvioimisessa ja tulevaisuuden suuntauksien vaikutusten kartoittamisessa on käytetty apuna sekä alan teknistä kirjallisuutta että identiteetin- ja pääsynhallinnan asiantuntijoilla teetettyä asiantuntijakyselyä.

Seuraavaksi kuvataan työn rakenne: johdannon jälkeen toisessa luvussa esitellään identiteetinhallinta yleisellä tasolla lähtien digitaalisesta identiteetin määrittelystä ja sen rakenteesta päätyen identiteetinhallinnassa toimivien eri osapuolten rooleihin ja lopulta identiteetin elinkaareen. Kolmannessa luvussa käsitellään identiteetinhallinnan ja pääsynhallinnan kannalta tärkeitä teknologioita, standardeja ja protokollia todentamisesta ja valtuuttamisesta federointiin, kertakirjautumiseen, identiteetin provisiointiin ja lopulta identiteettien hallinnointiin. Neljännessä luvussa esitellään nykyisiä identiteetinhallintajärjestelmiä alkaen korkean tason arkkitehtuuriesittelystä ja eri

komponenttien kuvauksesta päätyen tarjolla olevien identiteetinhallintatuotteiden esittelyyn ja keskinäiseen arviointiin. Viides luku sisältää osana työtä toteutetun asiantuntijakyselyn tulokset, joiden tarkoitus on esittää asiantuntijoiden näkemys identiteetinhallinnan teknologioiden nykytilasta sekä arvioida tulevaisuuden trendejä alalla. Kuudennessa luvussa käsitellään viidennen luvun kyselyn tulosten perusteella hyvin merkittäväksi arvioitua trendiä eli pilvipalveluja sekä sitä, miten niiden tuomat perinteiseen laskentaan verrattuna tuomat muutokset vaikuttavat identiteetinhallintaan. Seitsemäs luku kokoaa yhteen työstä tehdyt johtopäätökset.

2 Identiteetinhallinnan esittely

Tässä luvussa esitellään identiteetin- ja pääsyhallinnan peruskäsitteet. Aluksi käsitellään digitaalisen identiteetin luonnetta ja sen ominaisuuksia. Sitten esitellään identiteetin ja pääsynhallinnan eri toimijat sekä niiden roolit. Tämän jälkeen kuvataan identiteetin elämänkaaren vaiheet luomisesta poistamiseen.

2.1 Digitaalinen identiteetti

Identiteetinhallinnan käsittelyn kannalta on tärkeää ensin määritellä, mitä identiteetillä ja etenkin digitaalisella identiteetillä tässä yhteydessä tarkoitetaan. Arkikielessä sanaa identiteetti käytetään yleensä viittaamaan ihmisen käsitykseen omasta itsestään tai synonyyminä henkilöllisyydelle [1]. Molemmat merkitykset liittyvät osittain toisiinsa ja vastaavat kysymykseen, kuka tai mitä joku on. Niiden näkökulmat ovat kuitenkin erilaiset. Ensimmäisessä tulkinnassa on kyse henkilön sisäisestä käsityksestä itsestään, kun taas jälkimmäisessä ulkopuolisesta, muiden ihmisten, käsityksestä siitä kuka tai mitä joku on. Tässä työssä termiä identiteetti käytetään kuvaamaan jälkimmäistä tulkintaa eli henkilöllisyyttä, ja tarkemmin ottaen sen digitaalista muotoa.

Digitaalinen identiteetti voidaan määritellä digitaalisena esityksenä siitä informaatiosta, mitä jostain yksilöstä, organisaatiosta tai jostain muusta kohteesta tiedetään [2, s. 11]. Identiteetin omaava kohde voi olla henkilö, yritys, tietokone, sovellus, verkkoelementti tai lähes mitä tahansa [3, s. 8]. Identiteetin määrittävä informaatio voidaan jakaa kolmeen luokkaan [4, s. 5]:

- Tunnisteet (engl. identifiers)

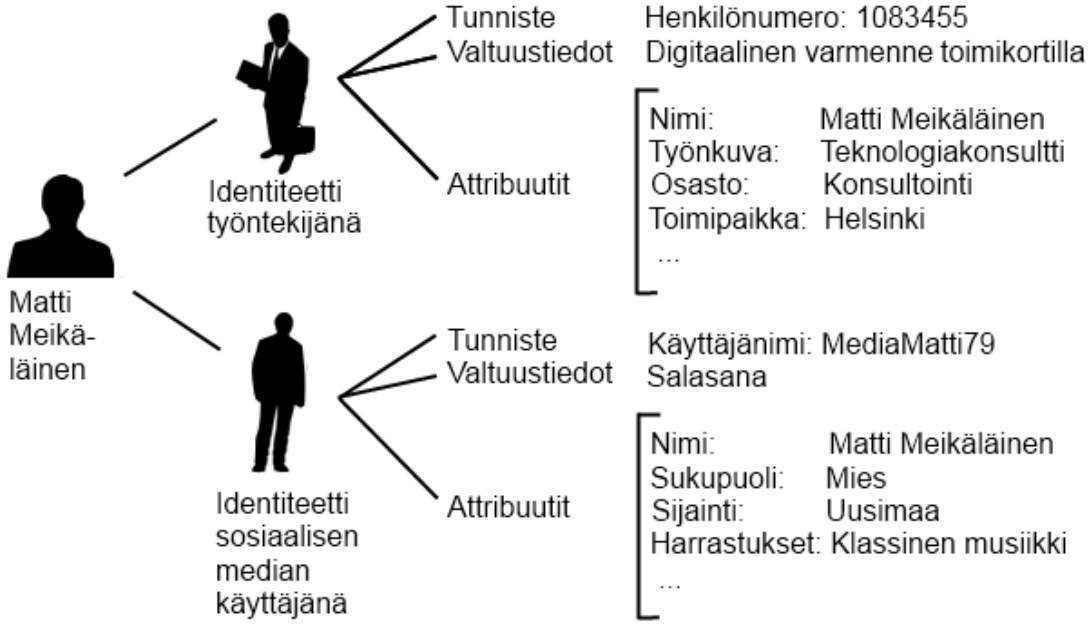
  Tunnisteet ovat numero-, merkki- tai symbolisarjoja, tai minkä tahansa muun muotoista informaatiota, joilla jokin kohde voidaan yksilöidä. Nämä tunnistettavat kohteet voivat olla esimerkiksi käyttäjiä, verkkoelementtejä, toimintoja, palveluita tai muita fyysisiä tai loogisia entiteettejä. [4, s. 2] Tunnisteet voivat olla luonteeltaan globaaleja eli täysin yksilöllisiä useiden eri järjestelmien ja/tai organisaatioiden halki, tai sitten täysin järjestelmäkohtaisia pseudonyymejä, joilla on vain paikallinen yksilöllisyys. Kahdella eri käyttäjällä voi siis eri yrityksissä olla täysin sama käyttäjätunnus, mutta heidän sähköpostiosoitteensa eivät siitäkään huolimatta voi olla samat, koska sähköpostiosoite on globaali tunniste siinä missä käyttäjänimi on vain paikallinen. Tunnisteiden pätevyys voi olla myös ajallisesti rajoitettu, jopa ainoastaan yhden istunnon tai transaktion pituiseksi. Esimerkkejä tunnisteista ovat muun muassa käyttäjänimet, sähköpostiosoitteet, puhelinnumerot, IP-osoitteet ja URI:t. [4, s. 15]

- Valtuustiedot (engl. credentials)

  Valtuustieto on informaatiota, jolla kohde voidaan todentaa (engl. authenticate) väittämäkseen kohteeksi ja jolla kohteen pääsyoikeudet voidaan valtuuttaa [4, s. 3]. Valtuustietoja voivat olla esimerkiksi käyttäjänimi-salasana-parit, varmenteet, älykortit tai biometriset tunnisteet. [4, s. 16].

- Attribuutit (engl. attributes)

Attribuutit ovat kohteeseen sidottua kuvailevaa informaatiota, joka määrittelee kohteen ominaisuudet [4, s. 2]. Tällaista informaatiota ovat esimerkiksi nimi, ikä, osoite, puhelinnumero. Attribuutit voivat myös sisältää oikeuksia, käyttöoikeuksia, delegointilistoja sekä erilaisia rajoituksia. Ne voivat myös sisältää tilannekohtaista tietoa kuten epäonnistuneiden kirjautumisten määrän. [4, s. 15]



Kuva 1: Esimerkki identiteettien sisältämästä informaatiosta luokittain [2, kuva 2.1., piirretty uudestaan]

Edellä kuvattuja identiteettitiedon kolmea luokkaa ja niiden keskinäisiä suhteita on havainnollistettu kuvassa 1. Kuvassa olevalla mallihenkilöllä on kaksi erilaista digitaalista identiteettiä - toinen työntekijänä ja toinen sosiaalisen median käyttäjänä. Kummatkin rakentuvat erilaisista identiteettitiedoista, mikä antaa hyvän mahdollisuuden vertailla erilaisia tunnisteita, valtuustietoja ja attribuutteja keskenään.

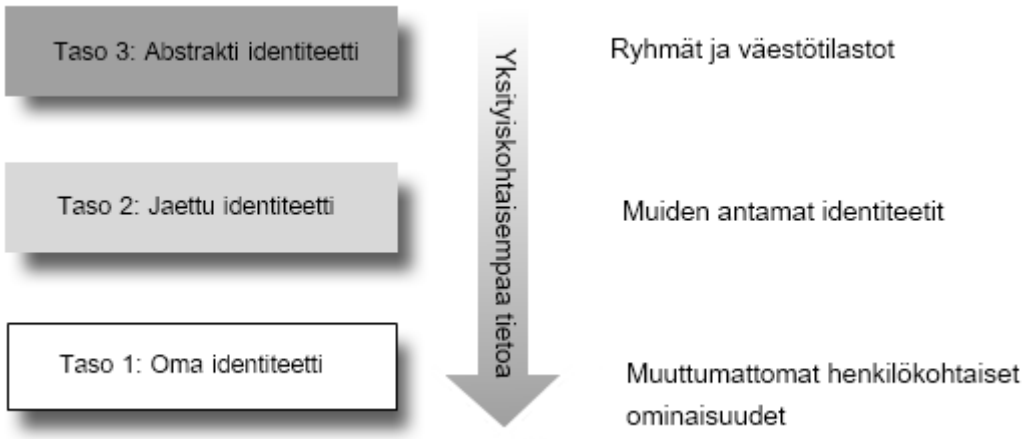
Toisin kuin arkikielessä yleensä, yhdellä kohteella voi olla useita eri identiteettejä. Nämä eri identiteetit ovat ikään kuin eri näkökulmia tai otoksia kohteeseen liittyvästä informaatiosta. [3, s. 12] Vaikka kuvan 1 identiteeteillä ei ole juuri mitään tekemistä keskenään, ne kuvaavat silti samaa kohdetta, Matti Meikäläistä. Kummatkin jakavat toki yhteisen nimi-attribuutin, mutta kyse ei ole siitä. Matti olisi voinut laittaa sosiaalisen median profiilissaan nimekseen minkä tahansa keksityn nimen ja identiteetit viittaisivat siitä huolimatta Mattiin. Eri identiteetit liittyvät siis toisiinsa viime kädessä ainoastaan yhteisen kohteensa kautta [3, s. 12].

Toisistaan täysin poikkeavien identiteettien olemassaoloa auttaa selventämään ne mekanismit, joilla identiteetit ylipäätään syntyvät. Identiteetit voidaan jakaa karkeasti kolmeen tasoon sen perusteella, miten ne muodostuvat ja kuinka yksityiskohtaista tietoa ne sisältävät. Taso 1 koostuu niistä lähes muuttumattomista ominaisuuksista, joita kohteella on [3, s. 12] kuten esimerkiksi syntymäaika, etnisyys ja biometriset ominai-

suudet kuten silmän iiris. Nämä ovat kaikista tarkimmin ja yksityiskohtaisimmin yksilöiviä tietoja.

Taso 2 kuvaa sellaisia identiteettejä, jotka muut tahot myöntävät jollekin kohteelle. Tämän tason jaetut identiteetit ovat väliaikaisia ja perustuvat jollekin sopimukselle tai suhteelle tahon ja kohteen välillä. Jaettu tarkoittaa tässä sitä, että identiteetti on olemassa keskinäisellä sopimuksella ja jos kumpikaan osapuoli peruu sopimuksen, identiteetti raukeaa. Esimerkiksi ajokortit, passit, luottokortit ja kirjastokortit ovat tällaisia identiteettejä. [3, s. 12]

Taso 3 kuvaa lähinnä joukkoidentiteettejä, jotka määräytyvät abstraktisti, eivätkä ole täsmällisiä tai yksityiskohtaisia [3, s. 12]. Ne ovat ikään kuin väestötieteellisiin tai muihin löyhiin ryhmiin perustuvia leimoja. Esimerkkejä tällaisista identiteeteistä ovat muun muassa ”helsinkiläinen”, ”50-vuotias mies”, ”keskituloinen” tai ”purjehdusta harrastava”.



Kuva 2: Identiteettien eri yksityiskohtaisuustasojen luokittelu [3, kuva 2.3, piirretty uudestaan]

Yhteenvetona digitaaliset identiteetit koostuvat siitä tiedosta, mitä jostain kohteesta on kerätty. Tämä identiteettitieto jakautuu kolmeen eri kategoriaan: tunnisteisiin, valtuustietoihin ja attribuutteihin. Tunnisteilla kohde voidaan yksilöidä, valtuustiedoilla kohde voidaan todentaa ja valtuuttaa, ja attribuuteilla kohdetta voidaan kuvailla sekä asettaa sille oikeuksista ja rajoituksista. Yhdellä kohteella voi myös olla useita eri identiteettejä, jotka voivat olla eri tasoisia riippuen siitä tavasta miten on myönnetty. Tällaiset identiteetit voidaan myöntää perustuen kohteiden muuttumattomiin ominaisuuksiin, erilaisiin sopimuksiin ja jäsenyyksiin perusten sekä myös löyhien väestötieteellisten tai ryhmätietojen perusteella.

2.2 Identiteetinhallinnan eri roolit

Tämä luku esittelee identiteetinhallinnassa vaikuttavia eri rooleja ja miten ne toimivat keskenään. Nämä roolit koostuvat kohteista, identiteetintarjoajista, palveluntarjoajista ja kontrolliosapuolista. Luvussa kuvataan ensin eri roolit ja niiden tehtävät ja lopuksi käsitellään vielä niiden keskinäisiä suhteita ja yhteistä toimintaa.

2.2.1 Kohteet

Kohteet ovat osapuolia, joiden identiteettiattribuutteja tallennetaan digitaalisesti ja käytetään transaktioihin tai muihin tarkoituksiin. Identiteettiattribuutit voidaan luokitella seuraavasti: [2, s. 25]

- Valtion myöntämät attribuutit

  Valtion myöntämät attribuutit toimivat perustana valtiolliselle identiteetille eli henkilöllisyydelle. Ne luodaan myönnettäessä erilaisia valtiollisia henkilöllisyysdokumentteja kuten passeja, syntymätodistuksia ja henkilökortteja. Koska valtion myöntämiä henkilöllisyysdokumentteja pidetään yleisesti kaikista vahvimpina todisteina henkilöllisyydestä, täytyy niiden attribuutit suojata vahvasti. Esimerkkejä näistä attribuuteista ovat esimerkiksi passinumerot ja sosiaaliturvatunnukset. [2, s. 25]

- Väestötieteelliset attribuutit

  Väestötieteelliset attribuutit kuvaavat suuripiirteisiä väestöllisiä ominaisuuksia kuten ikää, sukupuolta, asuinpaikkakuntaa jne. Vaikka nämä attribuutit ovat hyvin suurpiirteisiä, eivätkä yksittäisinä mahdollista yksilöintiä, yhdistelemällä näitä tietoja keskenään voi silti olla mahdollista yksilöidä yksittäisiä kohteita. [2, s. 25–26] Esimerkiksi jollain paikkakunnalla ei välttämättä ole kuin yksi 95-vuotias nainen, jolloin paikkakuntatieto, ikä ja sukupuoli yhdistettynä osoittavat tähän tiettyyn yksittäiseen kohteeseen.

- Taloudelliset attribuutit

  Taloudelliset attribuutit ovat yleensä pankkien ja muiden finanssiyritysten myöntämiä. Ne liittyvät usein rahaliikenteen käsittelyyn, mikä tekee niistä paitsi usein käytettyjä myös hyvin houkuttelevia kohteita varkauksille ja muille väärinkäytöksille. Tästä syystä näitä attribuutteja on suojattava ja useimmat finanssiyritykset ovatkin asettaneet turvamekanismeja väärinkäytöksien varalta. Esimerkkejä taloudellisesta attribuuteista ovat muun muassa luottokortti- ja tilinumerot. [2, s. 26]

- Biometriset attribuutit

  Biometriset attribuutit perustuvat ihmisten fyysisiin ominaisuuksiin kuten sormenjälkiin tai silmän iirikseen. Koska ne perustuvat fyysisiin yksilöllisiin eroihin, ne mahdollistavat hyvin vahvan todentamisen. Niiden käyttöön liittyy kuitenkin ongelmia, koska biometristen attribuuttien lukeminen ei ole vielä aivan kypsää teknologiaa ja siinä tapahtuu helposti virheitä. [2, s. 26]

- Transaktiokohtaiset attribuutit

  Transaktiokohtaiset attribuutit ovat hyvin dynaamisia ja kuvaavat niitä vuorovaikutuksia, joissa kohteet ovat osallisena Internetissä. Niitä voidaan käyttää esimerkiksi räätälöityjen palvelujen sekä kohdennetun markkinoinnin tarjoamiseen. Jos näitä attribuutteja ei kuitenkaan suojata riittävän hyvin, voivat ne paljastaa yksityisiä tietoja kuten esimerkiksi kohteen ajanvietto- ja kulutustottumuksia. [2, s. 26]

2.2.2 Identiteetintarjoajat

Identiteetintuottajat ovat yleisesti niitä osapuolia, jotka myöntävät ja hallinnoivat kohteiden identiteettejä. Ne suorittavat neljään perustoimintoa: [2, s. 27]

1. Luoda ja asettaa identiteettiattribuutit tietylle kohteelle;
2. Sitoa kohteen identiteettiattribuutit muihin saman kohteen identiteettiattribuutteihin;
3. Luoda vakuutukset (engl. assertions) identiteettiattribuuteista;
4. Myöntää käyttövaltuudet, jotka pohjautuvat näihin identiteettiattribuutteihin ja vakuutuksiin. [2, s. 27]

Identiteetintarjoajat voivat myös sitoa luomiansa ja myöntämiänsä identiteettiattribuutteja toisilta identiteetintarjoajilta saamiinsa identiteettiattribuutteihin. [2, s. 27] Esimerkiksi pankin myöntämä tilinumero voidaan sitoa valtion myöntämään sosiaaliturvatunnukseen ja nimiattribuutteihin, minkä jälkeen näiden kahden identiteetin - pankin myöntämän asiakasidentiteetin ja valtion myöntämän henkilöllisyyden - välille muodostuu riippuvuus.

Koska identiteetintarjoajat joutuvat luottamaan toisten identiteetintarjoajien antamiin valtuustietoihin ja attribuutteihin, on tärkeää että niillä on prosesseja, joilla arvioida identiteettitietojen varmuutta (engl. assurance). Tällaiset prosessit mahdollistavat jonkin luottamuksen asteen tai luottamustason asettamisen jollekin identiteettitiedolle. Asetettu luottamustaso voi pohjautua esimerkiksi sille, miten tarkka identiteetintarjoaja on ollut varmistaessaan ja asettaessaan attribuutteja tai luodessaan vakuutuksia niistä. [2, s. 27]

2.2.3 Palveluntarjoajat ja kontrolliosapuolet

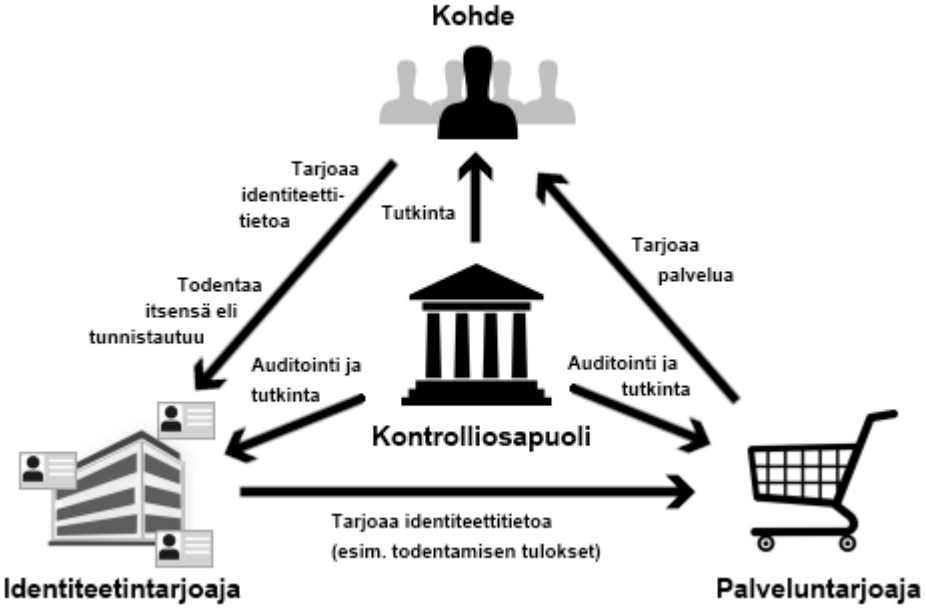
Palveluntarjoajat ovat osapuolia, jotka tarjoavat käyttäjille (tai käyttäjien puolesta toimiville agenteille) palveluja tai pääsyn resursseihin, jotka edellyttävät tiettyjä valtuustietoja käyttäjältä [2, s. 27]. Palveluntarjoajan kannalta onkin tärkeää päätellä, miten pitkälle ne voivat luottaa mihinkin valtuustietoihin sekä niiden attribuuttien ja vakuutuksien oikeellisuuteen. Osa palveluista voidaan tarjota matalamman varmuuden (engl. assurance) valtuustiedoilla, mutta osa edellyttää selvästi korkeampaa varmuustasoa. [2, s. 28]

Kontrolliosapuolet ovat tyypillisesti valtion valvontavirastoja ja säätelyelimiä, joiden tarvitsee päästä käsiksi identiteettitietoihin suorittaakseen tutkinnallisia ja valvonnallisia tehtäviä. [2, s. 28] Suomessa tällainen osapuoli voisi olla esimerkiksi viestintävirasto, joka tarvitsee pääsyn jonkin palveluntarjoajan identiteettitietojenkäsittelylokeihin valvoakseen lainmukaista henkilötietojen käsittelyä. Toisena esimerkkinä poliisi voi tarvita pääsyn telepalveluntarjoajan tallentamiin teletunnistetietoihin tutkiakseen rikosta.

2.2.4 Osapuolten väliset suhteet

Kaikki identiteetinhallinnan osapuolet toimivat jonkinlaisessa suhteessa toisiinsa, mutta niiden roolijako ei välttämättä ole täysin staattinen. Yksittäinen osapuoli voi esimerkiksi toimia sekä identiteetintarjoajana että palveluntarjoajana. Kohteet voivat

myös toimia identiteetintarjoajina joillekin identiteeteistään. [2, s. 28] Kontrolliosapuolien tehtävä on lähinnä valvoa muita identiteetinhallinnan osapuolia. Eri osapuolten suhteita on havainnollistettu kuvassa 3.



Kuva 3: Identiteetinhallinnan osapuolten keskinäiset suhteet [2, kuva 2.2, piirretty uudestaan]

Perinteisesti palveluntarjoajat ovat hoitaneet oman identiteetinhallintansa, mikä on johtanut siihen, että kohteilla on omat käyttäjänimensä ja salanansa jokaiselle palvelulle. Tämä taas on edellyttänyt myös kohteilta jonkinlaista identiteetinhallintaa, koska eri käyttäjänimi-salasana-pareista on pidettävä kirjaa. [2, s. 28]

Identiteetintarjoajan roolin tarkoitus on poistaa identiteetinhallinnan taakkaa kohteilta ja palveluntarjoajilta ja ottaa se omalle vastuulleen. Tällöin kohteiden ei tarvitse esimerkiksi hallita useita salanoja ja käyttäjänimiä, vaan ainoastaan identiteetintarjoajan tiliä. Palveluntarjoajien ei puolestaan tarvitse toteuttaa ja ylläpitää omia identiteetinhallinnan järjestelmiä, vaan ne voivat siirtää nämä tehtävät identiteetintarjoajalle ja keskittyä enemmän tarjoamaansa palveluun. Tehtävien myötä myös osa identiteetinhallintaan liittyvästä vastuusta siirtyy pois palveluntarjoajien harteilta, mikä helpottaa entisestään palvelun tarjoamiseen keskittymistä. [2, s. 28] Lisäksi, koska yksi identiteetintarjoaja voi palvella lukuisia palveluntarjoajia, identiteetinhallintajärjestelmän kokonaiskustannukset jakautuvat palveluntarjoajien kesken. Tämä tarkoittaa, että identiteetintarjoaja pystyy tarjoamaan kehittyneempiä identiteetinhallintapalveluja kuin palveluntarjoajat yksittäin voisivat toteuttaa vastaavalla kustannuksella. Tällaisia palveluita ovat muun muassa vahva todennus kuten verkkopankkitunnistautuminen sekä kertakirjautuminen. [2, s. 28]

2.3 Identiteetin elinkaari

Identiteetin elinkaarella tarkoitetaan yleisesti niitä vaiheita, joita identiteetit käyvät läpi olemassaolonsa eri vaiheissa. Nämä vaiheet voidaan jakaa neljään ryhmään: luomiseen eli provisiointiin, käyttöön, päivittämiseen ja käytöstä poistamiseen eli depro-

visiointiin. Näiden neljän vaiheen lisäksi on myös yksi jatkuva-aikainen osa identiteetin elinkaarta eli hallinnointi. [2, s. 29] Kokonaisuutena identiteetin elinkaarta voidaankin pitää jatkuvana prosessina, jossa saman kohteen yhden identiteetin loppua voi seurata toisen luominen jne. Tätä prosessia on kuvattu kuvassa 4. Ennen kuin siirrytään näihin neljään elämänkaaren vaiheeseen sekä hallinnointiin, selitetään ensin miten identiteetin luomisprosessi tapahtuu.

Kuva 4: Identiteetin elämänkaari [2, kuva 2.3, piirretty uudestaan]

2.3.1 Identiteetin luomisprosessi

Identiteetin luomisen voidaan ajatella koostuvan kolmesta vaiheesta: attribuuttien varmistamisesta, valtuustietojen myöntämisestä ja lopulta varsinaisen identiteetin muodostamisesta. Attribuuttien varmistaminen tarkoittaa jonkin luotetun tahon, esimerkiksi viranomaisten, todistusta käytettävien attribuuttien oikeellisuudesta. Tällainen luotettavaan auktoriteettiin perustuva attribuuttien varmistaminen on tärkeää, etenkin kun käsitellään rahaliikennettä. Toisaalta vähemmän säädellyt palvelut, kuten sähköpostipalvelu, saattavat yksinkertaisesti luottaa siihen, että käyttäjän syöttämät attribuutit ovat oikeat ilman virallisia todisteita. [2, s. 30]

Kun attribuutit on varmistettu, voidaan siirtyä valtuustietojen myöntämiseen. Riippuen valtuustiedon tyypistä, niitä voi myöntää joko jokin auktoriteetti tai kohde itse. Ensimmäisessä tapauksessa kyse voi olla esimerkiksi digitaalisesta varmenteesta, jonka myöntää yleensä joko organisaatio itse tai jokin ulkoinen luotettu osapuoli. Myös organisaation kuvallinen henkilökortti lukeutuu ensimmäiseen kategoriaan. Jälkimmäisessä tapauksessa tyypillisin esimerkki lienee salasana, jonka käyttäjä itse valitsee. Näille eri valtuustiedoille voidaan asettaa eri luottamustasoja niiden luotettavuuteen perustuen. Luotettavuuden arviointia varten on käytetyn valtuustietotyypin lisäksi keskeistä, että valtuustietoon on sidottu sen myöntäjä, myöntämispäivämäärä ja voimassaoloaika. [2, s. 31]

Valtuustietojen myöntämisen lisäksi tarvitaan vielä jokin tunniste, kuten henkilönumero tai käyttäjänimi, jotta identiteetti voidaan muodostaa. Tunnisteita asettaessa on hyvä huomioida nimiavaruuden riittävyys konfliktien välttämiseksi. Lisäksi mikäli käyttäjien on tarkoitus käyttää tunnistetta suoraan, tulisi tunnisteen olla lyhyt ja helposti muistettava sekä helposti kirjoitettava. [2, s. 31]

Kun kaikki identiteetin luomisvaiheet yhdistetään kokonaisuudeksi, voidaan esimerkkinä käyttää uuden työntekijän työhönottoa. Aluksi henkilöstöhallinta (HR) varmistaa työntekijän henkilötiedot eli attribuutit ja syöttää ne henkilöstönhallintajärjestelmään. Järjestelmä asettaa identiteetin tunnisteeksi esimerkiksi työntekijän henkilönumeron. Tämän jälkeen HR myöntää uudelle työntekijälle kuvallisen henkilökortin ja kulkukortin, jotka molemmat toimivat eri valtuustietoina. Siinä missä henkilökortti oikeuttaa henkilön oleskelemisen työpaikan yleisillä alueilla, voi kulkukortti sisältää lisäksi lisäoikeuksia rajatummille alueille. Tässä vaiheessa työntekijälle on luotu jo yksi identiteetti, mutta useimmissa työpaikoissa niitä luodaan vielä lisää. Yhteistyössä IT-hallinnon kanssa työntekijälle luodaan uusi identiteetti, jolla tämä voi tunnistautua yrityksen sisäisiin verkkopalveluihin. Identiteetin tunnisteen eli käyttäjänimen, myöntää joko IT-hallinto tai HR, mutta valtuustietona toimivan salasanan luo työntekijä itse. Tämä identiteetti jakaa todennäköisesti useita attribuutteja työntekijän aiemmin luodun identiteetin kanssa, mutta sisältää myös täysin omia attribuutteja, jotka liittyvät esimerkiksi käyttäjän asetuksiin eri sovelluksissa tai palveluissa. Todellisessa maailmassa työntekijälle voidaan toki joutua luomaan vielä lukuisia muitakin identiteettejä riippuen organisaation käyttämistä järjestelmistä ja politiikoista.

2.3.2 Provisiointi, identiteetin luominen ja välittäminen

Provisiointi on elinkaaren ensimmäinen askel ja käsittää identiteettien luomisen sekä identiteettitiedon välittämisen edelleen eri kohdejärjestelmille [5, s. 2]. Provisiointiin kuuluva identiteettien luomisen prosessi on jo kuvattu vaiheittain luvussa 2.3.1, joten tämä luku keskittyy automaattiseen provisiointiin sekä identiteettitiedon välittämiseen.

Provisioinnilla voidaan automaattisesti luoda identiteettejä suoraan jostain lähdejärjestelmästä, kuten henkilöstönhallintajärjestelmästä tai mistä tahansa lähteestä, joka sisältää tarvittavat identiteettiattribuutit kohteelle, esimerkiksi verkkopalvelun rekisteröintilomakkeesta [3, s. 30]. Tämä säästää merkittävästi manuaalista työtä ja nopeuttaa uuden identiteetin käyttöönottoa, mikä tehostaa esimerkiksi työhönottoa, kun potentiaalista työaikaa ei hukata erilaisia tunnuksia ja muita käyttöresursseja odotellessa [5, s. 2]. Verkkopalveluesimerkin tapauksessa identiteetin voi luoda jopa täysin itsepalveluna ilman, että palvelua ylläpitävä organisaatio tekee lainkaan työtä sen eteen [3, s. 30].

Kun kohteelle on luotu identiteetti, täytyy sen tiedot välittää oleellisilta osin kaikille sen tietoja käyttäville kohdejärjestelmille, jotta sitä voidaan alkaa käyttää. Kohdejärjestelmillä tarkoitetaan tässä kaikkia sovelluksia, tietojärjestelmiä tai muita resursseja, jotka tarvitsevat identiteettitietoja ja joihin nämä tiedot voidaan ja halutaan välittää. Esimerkkejä kohdejärjestelmistä ovat muun muassa käyttöjärjestelmä, sähköpostijärjestelmä, palkanlaskentajärjestelmä tai vaikkapa sähköinen tilausjärjestelmä, joka tilaa työntekijälle työsuhdepuhelimen ja -tietokoneen. [5, s. 2] Kohdejärjestelmiä voi yhden organisaation sisällä olla kymmeniä, tai jopa satoja, jolloin provisioinnin automaattisen identiteettitietojen välittämisen merkitys kasvaa.

Automaattisella identiteettitietojen provisioinnilla on myös tärkeä rooli identiteettien päivittämisen (ks. luku 2.3.4) yhteydessä, sillä ilman sitä on vaikea saavuttaa tietojen yhtenäisyyttä ja ajantasaisuutta eri kohdejärjestelmien välillä. Joka kerta kun jonkin identiteetin jokin attribuutti tai valtuustieto muuttuu, pitää muutos välittää kaikille kohdejärjestelmille. Jos sekä identiteettejä että kohdejärjestelmiä on lukuisia, tulee päivitysten määrästä niin suuri, että sen hoitaminen manuaalisesti alkaa muuttua kustannustehottomasta mahdottomaksi. Nämä kaikki automaattisen provisioinnin tuomat hyödyt ja säästöt ovat tehneet siitä hyvin suositun toiminnallisuuden yritysmaailmassa. [3, s. 30].

Yhteenvetona provisiointiärjestelmät nopeuttavat ja parantavat yleisesti organisaation sisäisiä prosesseja. Oikein asetettu provisiointijärjestelmä mahdollistaa sen, että uudet työntekijät voivat saada tarvitsemansa käyttäjätilit ja käyttöoikeudet työtehtävänsä edellyttämiin sovelluksiin ja järjestelmiin jopa ensimmäisenä työpäivänään, eikä työaikaa mene hukkaan turhaan odotteluun. Samalla provisiointi säästää myös henkilöstöhallinnan ja IT-hallinnan työaikaa, koska käyttäjätietoja ei tarvitse välittää käsin monelle eri taholle, eikä käyttäjätilejä luoda tai käyttöoikeuksia manuaalisesti asettaa kaikille käyttäjille. Nämä hyödyt eivät koske ainoastaan uuden työntekijän työhönottoa, vaan myös jokaista muutosta, joita olemassa oleviin käyttäjäidentiteetteihin tulee.

2.3.3 Identiteetin käyttäminen

Luodun identiteetin käyttäminen on ehkä helpoimmin ymmärrettävä vaihe identiteetin elinkaaressa. Kohteet käyttävät identiteettejään muun muassa eri järjestelmiin tunnistautumiseen ja oikeuttavat niillä eri toimintoja. [3, s. 31] Käyttäjä voi esimerkiksi kirjautua työpaikkansa sisäverkkoon ja kirjata työtuntinsa tuntiseurantajärjestelmään. Identiteettien käyttö mahdollistaa myös luotetun viestinnän, koska viestinnän osapuolet voivat etsiä ja löytää sekä varmentaa muiden identiteettejä [2, s. 32]. Esimerkiksi sähköpostit voidaan allekirjoittaa digitaalisesti, jotta identiteeteistä voidaan varmistua, ja lisäksi viestit voidaan vielä salata, jos halutaan varmistua niiden luottamuksellisuudesta. Viestinnän lisäksi muut tahot voivat käyttää muiden kohteiden identiteettejä suorittaakseen omia tehtäviään. Tällaisia tahoja ovat esimerkiksi palkanlaskenta, laskutus, kulunvalvonta jne. [3, s. 31].

Vaikka kaikki mitä identiteetin käyttämisestä on kirjoitettu yllä koskee ihmiskohteita, pätevät samat tosiasiat myös laitteiden, sovellusten tai muiden elottomien kohteiden näkökulmasta [3, s. 31]. Laite voi tarvita identiteettiä, jotta se voi tunnistautua esimerkiksi verkkoon tai palveluun ja suorittaa siellä identiteetin sallimia toimintoja. Laitteet ja sovellukset tarvitsevat identiteettejä niin ikään löytääkseen toisensa ja kommunikoidakseen luotetusti keskenään. Samoin laite- ja sovelluskohteiden ulkopuoliset tahot, kuten valvonta- ja raportointijärjestelmä, käyttävät kohteiden identiteettejä seurantaan samaan tapaan kuin henkilöstönhallinta tarvitsee työntekijöiden identiteettejä tuntiseurantaan.

2.3.4 Identiteetin päivittäminen

Kaikkia identiteettejä joudutaan ajoittain päivittämään, koska osa attribuuteista muuttuu ajan myötä - roolit, työnkuvat, osoitteet, puhelinnumerot, sähköpostiosoitteet ja monet muutkin attribuutit voivat muuttua useitakin kertoja identiteetin olemassaolon aikana [3, s. 31–32]. Attribuuttien muutokset voivat vaikuttaa myös valtuustietoihin [2, s. 34]. Esimerkiksi roolin tai työnkuvan vaihtuessa, kohde voi menettää joitain val-

tuuksia ja saada niiden tilalle uusia. Valtuustiedot vaativat päivittämistä myös riippumatta attribuuttien muutoksista, koska valtuustiedoille on usein asetettu jokin voimassaoloaika ja ne raukeavat, ellei niitä uusi.

Yleisesti kaikki päivitykset identiteetteihin tulisi tehdä viipymättä [2, s. 35], ettei syntyisi tilanteita, joissa kohteella ei esimerkiksi ole tehtäväänsä tarvittavaa oikeutta tai vielä pahemmassa tapauksessa kohteella on edelleen oikeus, jota sillä ei saisi olla. Toinen vältettävä tilanne on esimerkiksi tärkeän työpostin lähettäminen vanhaan osoitteeseen. Automaattinen provisiointi auttaa merkittävästi tämän ajantasaisuuden ja yhtenäisyyden saavuttamisessa (ks. luku 2.3.2) etenkin ympäristöissä, joissa sekä päivitettäviä identiteettejä että kohdejärjestelmiä on hyvin useita.

Tietojen ajantasaisuuden ohella tärkeää olisi myös pitää kirjaa kaikista muutoksista, joita identiteeteille tehdään. Tämä mahdollistaa sisäisen tutkinnan ja tarkastuksen pitkänkin ajan jälkeen tapahtumasta. Ilman kirjanpitoa voi olla vaikea osoittaa, että jollain henkilöllä on ollut jokin tietty valtuustieto jonain tiettynä hetkenä menneisyydessä, mikä on esimerkiksi mahdollistanut jonkin luvattoman toiminnon. Kirjanpitoon ja seurantaan liittyen on myös syytä varmistaa, että identiteetin pääasialliset tunnisteet kuten esimerkiksi henkilönumero, pysyvät muuttumattomana koko identiteetin elinkaaren ajan, koska kaikki muut osat identiteettiä voivat periaatteessa muuttua. [2, s. 35] Jos tunnistekin muuttuisi, voisi se johtaa tilanteisiin, joissa yhdestä identiteetistä on tullut täysin erillinen uusi identiteetti, eikä sitä voida enää yhdistää helposti aiempaan.

2.3.5 Identiteetin deprovisiointi

Deprovisiointiin liittyy läheisesti provisiointiin ja monissa yhteyksissä se jopa luetaan siihen sisältyväksi. Sen avulla käyttäjäidentiteettejä ja niiden tietoja voidaan poistaa, kun niiden elinkaari on tullut päätökseensä. [5, s. 2] Provisioinnin tapaan tiedot voidaan poistaa yhtenäisesti kaikista niistä kohdejärjestelmistä, joita käyttöoikeuden menetys koskettaa. Esimerkiksi työtehtävää vaihtanut työntekijä voidaan deprovisioida joistain kohdejärjestelmistä, ja vastaavasti provisioida joihinkin uuden toimenkuvan edellyttämiin uusiin kohdejärjestelmiin osan kohdejärjestelmäidentiteeteistä pysyessä ennallaan. Mikäli työntekijän työsuhde päättyy kokonaan, voidaan hänen identiteettinsä deprovisioida kaikista kohdejärjestelmistä. Turvallisuusnäkökulmasta deprovisiointia voidaankin pitää tärkeämpänä toimintona kuin provisiointia [5, s. 2]. Tämä johtuu siitä, että entiset (ja nykyiset) työntekijät, joilla on pääsy resursseihin, joihin heillä ei sitä pitäisi enää olla, ovat mahdollinen tietoturvauhka siinä missä työntekijät ilman käyttäjätunnuksia yleensä vain laskevat työtehokkuutta [5, s. 2].

Ilman kohdejärjestelmien halki toimivaa deprovisiointia entiset työntekijät saattavat pystyä käyttämään joitain resursseja vielä vuosia työsuhteen loppumisen jälkeen. Lisäksi tällaiset "unohdetut" identiteetit mahdollistavat myös ulkoisten hyökkääjien huomaamattoman pääsyn järjestelmien sisään. [3, s. 32] Hukatut, varastetut tai paljastuneet valtuustiedot mahdollistavat niin ikään ulkopuolisten pääsyn rajoitettuihin resursseihin, jos identiteettejä tai niiden osia ei deprovisioida kunnolla tällaisen tapahtuman sattuessa. Nämä puutteellisen deprovisioinnin aiheuttamat riskit ovat yksiä merkittävimmistä tietoturvariskeistä, joita yrityksillä on [3, s. 32].

2.3.6 Identiteettien hallinnointi

Koko elinkaaren ajan kaikkia edellä listattuja identiteeteille tehtäviä toimintoja tulisi hallita selkeillä politiikoilla, joista tulee pitää myös kirjaa. Tämä identiteettien hallinnointi on tärkeä osa organisaationlaajuista sisäistä valvontaa ja se on sekä suunniteltava että suoritettava oikein, jotta kaikki vaatimustenmukaisuudet (engl. compliancies) saadaan täytettyä. [2, s. 36]

Identiteetinhallintaan liittyvät politiikat koskevat pitkälti varmennusta ja valtuutusta. Varmennuspolitiikat määrittelevät vaaditun varmuuden (engl. assurance) identiteetin kaikille toimille (engl. transaction). Nämä politiikat määrittelevät ne olosuhteet, joissa kohteiden annetaan käyttää identiteettiin pohjautuvia palveluja tai informaatiota. Jokaisella eri toimijalla voi olla omat identiteettipolitiikkansa. Ne voivat muun muassa määritellä kohteet, sijainnit joista yhteys saadaan muodostaa sekä sallitut ajankohdat yhteyksille. [2, s. 36]

Organisaatioiden identiteettipolitiikkoihin kuuluu yleensä myös tehtävien eriyttäminen (engl. segregation of duties) ja sen valvonta, joiden tarkoituksena on tarkistaa ajoittain, että jokaisella identiteetillä on vain ne oikeudet, jotka sille kuuluvatkin [6, s. 9]. Tällä tavalla voidaan havaita ja korjata tilanteita, joissa identiteetillä on tarpeettomia tai vaarallisia oikeusyhdistelmiä, tai joissa kokonaisia tarpeettomia identiteettejä on jäänyt järjestelmään. Näiden uhkatilanteiden ohella nämä tarkistukset auttavat myös työntekijöitä, joille ei jostain syystä ole myönnetty kaikkia tarvittavia oikeuksia.

Politiikoiden ohella on tärkeää pitää huolta, että jäljitysketjut (engl. audit trail) kirjataan kaikista identiteetteihin liittyvistä muutoksista ja toimista. Jäljitysketjut sisältävät yksityiskohtaiset, luotettavat ja todistettavat tiedot jokaisesta toimesta, johon identiteetit ovat olleet osallisena. Tällä tavoin voidaan ehkäistä kiistettävyyttä (engl. repudiation), koska toimet voidaan jäljittää tarkasti tiettyyn identiteettiin ja aikaan. Tätä varten jäljitysketjusta tulisi selvitä vähintään kohde, joka on pyytänyt tiettyä toimea, aika jolloin pyyntö on tehty, mitä tietoa on käsitelty ja mikä tarkoitus toimella oli. [2, s. 37]

Olivat identiteettipolitiikat ja jäljitysketjut kuinka tahansa hyvin toteutettu, ne edellyttävät aina valvontaa ja läpikäyntiä, jotta niistä olisi todellista hyötyä. Tämä voidaan toteuttaa valvonta- ja raportointityökaluilla, jotka tarkkailevat reaaliaikaisesti käyttöoikeuksia, identiteeteillä suoritettuja toimia ja identiteettipolitiikoiden, kuten esimerkiksi tehtävien eriyttämisen, toteutumista ja raportoivat poikkeamista. Ilman tällaista valvontaa ja raportointia, useat poikkeamat voidaan havaita liian myöhään esimerkiksi puolivuotisauditoinnin yhteydessä tai ne saattavat jäädä kokonaan havaitsematta. [7, s. 374–375]

2.4 Yhteenveto

Digitaaliset identiteetit ovat digitaalisia esityksiä tiedosta, joka kuvaa jotain kohdetta, kuten esimerkiksi ihmistä tai verkkolaitetta, ja sen oikeuksia. Osa näistä tiedoista on kerätty kohteen ominaisuuksista ja osa taas myönnetty identiteetintarjoajan taholta. Nämä tiedot jakautuvat attribuutteihin, valtuustietoihin ja tunnisteisiin. Attribuutit ovat kohdetta kuvailevia tietoja kuten esimerkiksi ikä tai asuinosoite ihmisen tapauksessa ja laitteen tapauksessa esimerkiksi valmistusnumero. Valtuustiedot myönnetään kohteelle, jotta kohde voidaan todentaa ja sen oikeudet valtuuttaa, esimerkiksi henkilön oikeus kirjautua sisään tietylle työasemalle salasanalla tai toimikortilla. Tunnisteet

ovat myös identiteetille myönnettäviä tietoja, joiden tarkoitus taas on yksilöidä eri identiteetit joko paikallisella tai globaalilla tasolla, esimerkiksi Suomen sosiaaliturvatunnus.

Identiteettien yleistä käsittelyä voidaan kutsua identiteetinhallinnaksi. Se koostuu käytännössä neljästä eri osapuolesta tai roolista. Kohteet ovat osapuolia, joiden tietoja kerätään ja joille luodaan identiteettejä, joita käytetään erilaisten toimintojen suorittamiseen. Esimerkiksi minkä tahansa valtion kansalaiset ovat kohteita, joista valtio on kerännyt tietoa ja myöntänyt heille identiteetin, jota sekä valtio että kansalaiset voivat käyttää erilaisiin tarkoituksiin. Edellisessä esimerkissä mainittu valtio suorittaa toista identiteetinhallinnan kannalta keskeistä roolia eli identiteetintarjoajaa – tahoa, joka myöntää ja hallinnoi identiteettejä. Muita esimerkkejä identiteetintarjoajista ovat työnantajat, osa palveluyrityksistä sekä yksityishenkilöt. Yksityishenkilöt yleensä myöntävät ja hallinnoivat lähinnä omia identiteettejään, esimerkiksi oman tietokoneensa käyttäjinä, jolloin he ovat sekä kohteita että identiteetintarjoajia samalle identiteetille. Palveluyritykset suorittavat usein myös kolmatta roolia eli palveluntarjoajaa, joka tarjoaa jotain palvelua tai resurssia todennetuille identiteeteille eli asiakkailleen. Neljäntenä roolina ovat kontrolliosapuolet, jotka käyttävät identiteettitietoja ja identiteettien käsittelytietoja suorittaakseen tutkintaa ja valvontaa. Monet tämän roolin suorittajista ovat valtion valvontavirastoja ja säätelyelimiä kuten esimerkiksi poliisi tai viestintävirasto.

Identiteetin elinkaari alkaa provisioinnilla, jossa kohteelle luodaan identiteetti varmistetuista attribuuteista, ja jonka jälkeen nämä identiteettitiedot välitetään edelleen kaikkiin kohdejärjestelmiin. Tämän jälkeen jokainen kohdejärjestelmistä voi tunnistaa kohteen ja tarjota sille pääsyä kaikkiin niihin palveluihin ja resursseihin, joihin kohteelle on määritetty oikeudet. Provisiointi tulee alun jälkeen kyseeseen myös elinkaaren varrella, kun kohteen identiteetin tiedot muuttuvat. Nämä muutokset tulee välittää kaikkiin kohdejärjestelmiin aivan samaan tapaan kuin elinkaaren alussakin. Päivittämisen lisäksi identiteettiä täytyy hallinnoida koko sen elinkaaren ajan. Sen tulee täyttää joka elinkaarensa vaiheessa identiteetinhallintapolitiikoiden asettamat vaatimukset ja kaikista identiteettiin tulevista muutoksista on pidettävä kirjaa, jotta sen ja siihen sidotun kohteen suhde ei hämärtyisi ajan kuluessa. Tämän tarkan suhteen ylläpitäminen liittyy usein erilaisten vaatimustenmukaisuuksien täyttämiseen kuten myös kaikista identiteetillä suoritetuista toimista kirjattava jäljitysketju. Jäljitysketjun tarkoitus on luoda kiistämättömyys identiteetin ja sillä suoritettujen toimien välillä, jotta sisäistä valvontaa ja tutkintaa voidaan suorittaa luotettavasti. Identiteetin elinkaaren päätteeksi identiteetti poistetaan eli deprovisioidaan. Deprovisiointi on kuin vastatoiminto provisioinnille ja sen tarkoitus on poistaa kokonaisia identiteettejä tai niiden osia kokonaisvaltaisesti kaikista kohdejärjestelmistä. Se on tietoturvanäkökulmasta hyvin tärkeä prosessi, koska sen laiminlyönti voi johtaa vakaviin tietoturvauhkiin.

3 Keskeiset teknologiat, standardit ja protokollat

Tämä luku käsittelee yleisimpiä identiteetin- ja pääsynhallinnassa käytettäviä teknologioita, standardeja ja protokollia. Luvussa käsitellään ensimmäisenä todennusta ja valtuuttamista, jotka ovat pääsynhallinnan kannalta hyvin keskeisiä toimintoja. Tämän jälkeen siirrytään ensin federointiin ja sitten kertakirjautumiseen. Nämä on käsitelty molemmat omissa luvuissaan merkityksellisyytensä vuoksi, vaikka ne voisi myös sijoittaa todentamisen alle. Näiden jälkeen vuorossa ovat provisiointiprotokollat, hakemistopalvelut sekä identiteettien hallinta.

3.1 Todennus ja valtuuttaminen

Tämä luku käsittelee todennusta ja valtuuttamista, jotka ovat läheisiä käsitteitä pääsynhallinnassa. Näitä käsitteitä on jo hieman avattu toisessa luvussa, mutta selvyyden vuoksi niiden roolit kerrataan vielä uudestaan. Todentamisella tarkoitetaan kohteen identiteetin varmistamista eli onko kohde se henkilö tai laite, joka se väittää olevansa. Valtuuttaminen puolestaan käsittelee identiteetille myönnettyjä käyttöoikeuksia, jotka kohde saa todentamisen jälkeen eli mitä kohde voi identiteettinsä suomana tehdä ja mitä ei. Luvussa käsitellään ensin yleisesti todennuksessa ja valtuuttamisessa käytettäviä valtuustietoja, minkä jälkeen esitellään niiden toteutuksessa käytettäviä standardeja ja protokollia.

Valtuustiedot

Valtuustiedot ovat pääasiassa todentamiseen ja valtuuttamiseen käytettäviä identiteettitietoja. Ne sisältävät identiteettiattribuutteja ja -vakuutuksia jostain kohteesta, jotka jokin identiteetintarjoaja on myöntänyt. Valtuustiedon myöntäjä on tärkeä arviointiperuste palveluntarjoajalle sen päättäessä hyväksyäkö vai hylätäkö kohteen tarjoama valtuustieto. Tämä perustuu siihen, että myöntäjä vahvistaa valtuustiedon sisällön oikeellisuuden sekä mahdollisesti myös sen kelpoisuuden (engl. validity). Oikeellisuus viittaa tässä yhteydessä siihen, ettei valtuustietoa ole päästy vääristelemään, ja kelpoisuus siihen, että valtuustiedon sisältämät tiedot ovat paikkansapitäviä. Kohteet voivat myöntää myös itselleen valtuustietoja, mikä on hyvin hyödyllistä etenkin sellaisissa palveluissa, joissa varmuusvaatimukset ovat pienet tai niitä ei ole lainkaan kuten esimerkiksi harrastussivustoilla. [2, s. 46]

Tunnetuimmat digitaaliset valtuustiedot ovat julkisen avaimen salaukseen (engl. public-key encryption) perustuvat varmenteet, jotka pohjautuvat ITU-T:n kansainväliseen X.509-standardiin [8]. Niissä kohteen identiteettiattribuutit on sidottu kohteen julkiseen salausavaimeen (engl. public key). Julkisen avaimen salauksen pääasiallinen tarkoitus on mahdollistaa salattujen viestien lähettäminen tietylle kohteelle ilman, että kohteen ja lähettäjän täytyy jakaa yhteistä salaista avainta. Koska jokaisen kohteen julkinen avain on yksilöllinen, niitä voidaan kuitenkin käyttää myös tunnisteina ja todentamiseen. Varmenteet koostuvat kohteen identiteettitiedoista, kohteen julkisesta avaimesta sekä varmenteen myöntäneen varmenneauktoriteetin (engl. certificate authority, CA) tunnistamiseen tarvittavista identiteettitiedoista. Lopuksi nämä kaikki tiedot on digitaalisesti allekirjoitettu varmenneauktoriteetin toimesta, salaamalla ne sen yksityisellä avaimella. [2, s. 49–50]

Kohteet voivat myös delegoida valtuustietoja toisilleen. Tämä tarkoittaa sitä, että kohde voi antaa toiselle kohteelle oikeuden käyttää joitain sen valtuustietoja. Tyypillisesti valtuustietojen delegointi koskee valtuutuksia sisältäviä valtuustietoja, jolloin kohde antaa valtuutuksensa toisen kohteen käyttöön. Tarve tällaiselle delegoinnille syntyy yleensä, kun kohteen B täytyy suorittaa joitain tehtäviä kohteen A puolesta ja tarvitsee tätä varten A:n valtuutuksia. [2, s. 52] Tilanne mutkistuu kuitenkin hieman kun kuvioon otetaan mukaan useampia kohteita, joilla ei ole kaikkiin muihin osapuoliin muodostettua luottamussuhdetta. Voidaan ajatella tilanne, jossa kohteella A on luottamussuhde B:hen ja C:hen, mutta B:n ja C:n välillä ei ole keskinäistä luottamusta. Jos B joutuu suorittamaan toimia C:n kanssa A:n puolesta, täytyy C:n voida jotenkin luottaa B:hen. Tilanteen voisi ratkaista esimerkiksi siten, että A lainaisi yksityisen salausavaimensa B:lle, mutta tämä ratkaisu on tietoturvan kannalta huono, koska A:n yksityinen avain ei enää olisi salainen ja luotettava. Tällöin kohde B voisi muun muassa esittää olevansa A ilman, että sitä voisi mitenkään erottaa A:sta itsestään. Toinen vaihtoehto olisi, että aina kun C saisi pyynnön B:ltä jossa B toimii A:n puolesta, C pyytäisi A:ta varmistamaan pyynnön aitouden. Tämä vaihtoehto voi kuitenkin olla raskas ja epäkäytännöllinen. [2, s. 53] Huomattavasti parempi vaihtoehto onkin, että A myöntää B:lle varmenteen, jossa vakuutetaan, että B:llä on valtuutus toimi A:n puolesta [2, s. 54]. C voi tarkistaa varmenteen olevan A:n allekirjoittama ja näin luottaa siihen. Tällaisella ratkaisulla kaikki osapuolet voivat toimia luotettavasti keskenään ilman tietoturvaa vaarantavia kompromisseja.

Security Assertion Markup Language (SAML)

Security Assertion Markup Language (SAML) 2.0[9] on XML-pohjainen avoin standardi todennus- (eng. auhtentication) ja valtuuttamistietojen (engl. auhtorization) välittämiseen eri tietoturvatoimialueiden (engl. security domain), kuten esimerkiksi palveluntarjoajan ja tunnistuslähteen, välillä. SAML-standardi ei määrittele miten itse todennus toteutetaan, vaan ainoastaan miten todennus- ja valtuuttamistiedot välitetään, kun todennus on tehty. SAML-standardin toiminta perustuu sarjaan XML-pohjaisia viestejä eli vakuutuksia (engl. assertion). Nämä vakuutukset voidaan jakaa kolmeen kategoriaan eli todennusvakuutuksiin (engl. authentication assertion), ominaisuusvakuutuksiin (engl. attribute assertion) ja valtuutusvakuutuksiin (engl. authorization assertion). Todennusvakuutukset kuvaavat, miten ja milloin vakuutuksen kohde on todennettu. Ominaisuusvakuutukset kuvaavat, mitä ominaisuuksia eli esimerkiksi rooleja, oikeuksia ja pääsyoikeuksia, vakuutuksen kohteeseen on sidottu. Valtuutusvakuutuksien tarkoitus puolestaan on kuvata, miten kohde voi käsitellä tietoja ja resursseja ominaisuusvakuutuksien kuvaamien roolien ja oikeuksien perusteella. Näiden vakuutuksien lähettämiseen SAML voi käyttää muun muassa HTTP-, SMTP-, FTP- sekä SOAP-protokollia. [10, s. 137][9, s. 11]

SAML-profiilit koostuvat kerrosmaisesta rakenteesta. Jokainen profiili vastaa tiettyjä toimintojen joukkoa kuten kertakirjautumista. Näiden toimintojen toteutukset on määritelty yhdistelminä sidoksista (engl. bindings), protokollista ja edellisessä kappaleessa mainituista vakuutuksista. Erilaiset yhdistelmät mahdollistavat erilaisia toteutuksia samasta profiilista. SAML 2.0 sisältää useita profiileja, joita on esitelty alla. [2, s. 80]

- *Kertakirjautumisprofiilit*, sisältäen muun muassa:

- *Internetselain-kertakirjautumisprofiili* määrittelee selaimella tapahtuvan kertakirjautumisen vaatimat toiminnot [2, s. 80].

- *Identiteetintarjoajanlöytämisprofiili* määrittelee toiminnot, joilla palveluntarjoajat voivat löytää identiteetintarjoajat [2, s. 81].

- *Kertauloskirjautumisprofiili (engl. single logout profile)* määrittelee toiminnot, joilla käyttäjät voivat kirjautua kerralla ulos kaikista palveluista, joihin he ovat kertakirjautuneet sisään [2, s. 81].

- *Artifaktien vaihto -profiili (engl. artifact resolution profile)* määrittelee toiminnot artifaktien eli viittauksia vakuutuksiin sisältävien pienien datapakettien, vaihtamiseen identiteetintarjoajien ja palveluntarjoajien välillä. Artifakteja on tarkoitettu käytettäväksi silloin kun identiteettitietoja ei voida suoraan vaihtaa esimerkiksi rajoitetun kaistanleveyden vuoksi. [2, s. 81]

- *Vakuutuksien kysely ja pyyntö -profiili (engl. assertion query and request profile)* määrittelee toiminnot, joilla palveluntarjoajat voivat hankkia SAML-vakuutuksia ei-kertakirjautumiskäytössä [2, s. 81].

- *Tunnisteiden kuvaus -profiili (engl. name identifier mapping profile)* määrittelee toiminnot, joilla palveluntarjoajat voivat hankkia kohteille tunnisteita, joita muut palveluntarjoajat voivat käyttää [2, s. 81].

SAML-sidokset määrittelevät SAML-protokollaviestien kuvauksen viestintäprotokollille kuten HTTP-protokollalle ja SOAP-protokollalle. Esimerkiksi SAML SOAP -sidos määrittelee miten SAML-viestejä voidaan koteloida (engl. encapsulate) SOAP-viestiformaatissa. Muita SAML-sidoksia ovat Reverse SOAP -, HTTP-uudelleenohjaus-, HTTP POST -, HTTP-artifakti- ja SAML URI -sidokset. [2, s. 81] Näistä sidoksista voi lukea lisää SAML-standardin määrittelystä [9].

SAML-protokollat määrittävät pyyntö-vastaus-pareja SAML-viestien ja -tietojen vaihtamista varten. Esimerkiksi todentamiseen liittyvä pyyntö-vastaus-pari on määritelty "AuthRequest"-"AuthResponse"-pariksi. SAML-protokollat itsessään ovat riippumattomia alemman tason tiedonsiirtoprotokollista kuten HTTP-protokollasta – kaikki riippuvuudet alempiin protokolliin määritellään SAML-sidoksissa. SAML-protokolla ovat vakuutuksien kysely ja pyyntö- (engl. assertion query and request protocol), artifaktien vaihto -(engl. artifact resolution protocol), todennuspyyntö- (engl. authentication request protocol), tunnisteidenhallinta- (engl. name identifier management protocol), kertauloskirjautumis- ja tunnisteiden kuvaus (engl. name identifier mapping protocol) -protokollat. [2, s. 82–83] Näistä protokollista voi lukea lisää SAML-standardin määrittelystä [9].

Open Authentication

Open Authentication (OAuth) [11] on todennusprotokolla, joka tarjoaa vaihtoehdon perinteiselle todennuksen asiakas-palvelin-mallille lisäämällä malliin valtuutuskerroksen (engl. authorization layer) ja erottamalla asiakaskoneen ja resurssin omistajan roolit toisistaan. Perinteisessä mallissa resurssin omistaja joutuu jakamaan valtuustietonsa asiakaskoneiden ja kolmansien osapuolien sovellusten kanssa, jotta ne saisivat pää-

syn suojattuun resurssiin. Tämä lähestymistapa tuo tullessaan useita turvallisuusriskejä, koska se esimerkiksi antaa tarpeettoman paljon oikeuksia kolmansille osapuolille, eikä omistaja voi perua pääsyoikeutta yksittäiseltä taholta perumatta sitä kaikilta. OAuth-protokolla pyrkii korjaamaan näitä ongelmia antamalla pääsynhallinnan kokonaan resurssin omistajalle, joka voi sitten jakaa erillisiä pääsyoikeuksia asiakaskoneille. [11, s. 4]

OAuth-protokollassa asiakaskoneet ja -sovellukset eivät saa käyttöönsä resurssin omistajan valtuustietoja päästäkseen käsiksi resurssiin, vaan valtuutuspalvelin jakaa niille omat pääsylipukkeensa (engl. tokens). Nämä pääsylipukkeet koostuvat merkkijonosta, joka määritellee pääsyoikeuden laajuuden, voimassaoloajan sekä muita attribuutteja. Resurssin omistaja hallinnoi pääsylipukkeiden myöntämistä. [11, s. 4] Käyttämällä jokaiselle asiakaskoneelle ja sovellukselle omaa pääsylipuketta, niitä voidaan sulkea yksittäisesti, eivätkä itse resurssin omistajan valtuustiedotkaan ole perinteisen mallin mukaisessa vaarassa.

Esimerkkinä OAuth-protokollan toimintaperiaatteessa voidaan ajatella tilannetta, jossa käyttäjä antaa tulostuspalvelulle pääsyn valokuviin, jotka on tallennettu valokuvienjakopalveluun. Käyttäjä todentaa itsensä valtuutuspalvelimelle ja antaa hyväksyntänsä pääsylipukkeen myöntämisestä tulostuspalvelulle. Valtuutuspalvelin antaa tulostuspalvelulle pääsylipukkeen, jolla tulostuspalvelu voi todentaa itsensä valokuvienjakopalvelun palvelimelle, ja käyttäjä saa tulostettua haluamansa kuvat. Koko prosessi onnistui ilman että käyttäjän tarvitsi paljastaa käyttäjänimeään ja salasanaansa tulostuspalvelulle. Käyttäjä toimi tässä esimerkissä resurssin omistajana, tulostuspalvelu asiakaskoneena ja valokuvienjakopalvelu resurssipalvelimena. [11, s. 4]

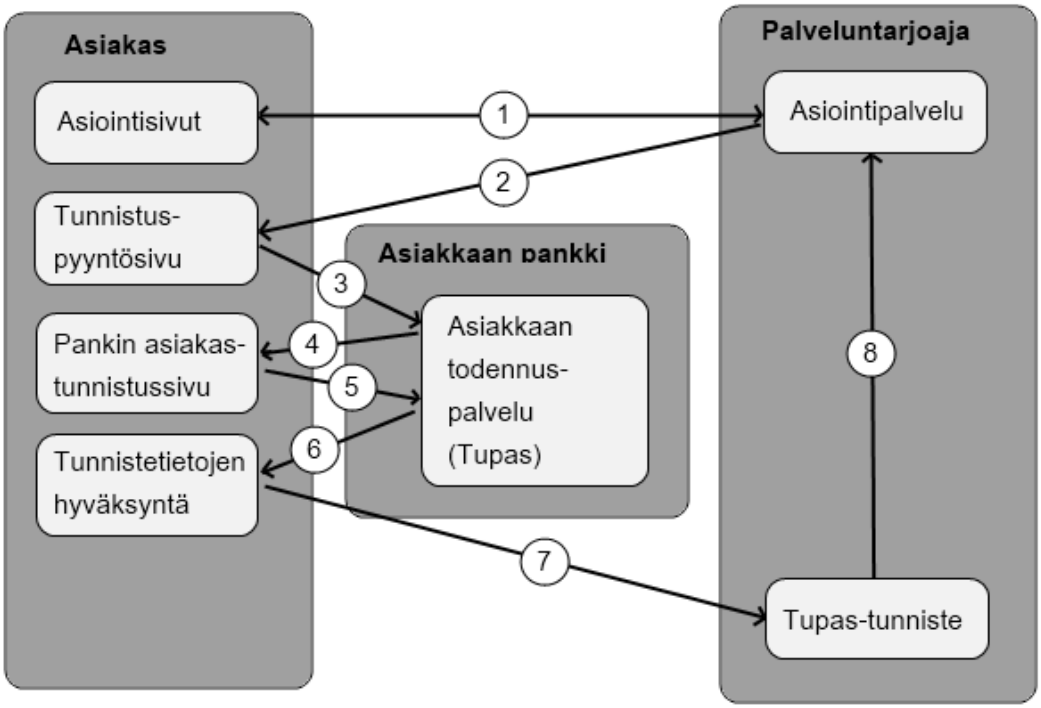
Yhteenvetona todentaminen ja valtuuttaminen ovat yksiä tärkeimmistä pääsynhallintaan liittyvistä toiminnoista. Todentaminen varmistaa kohteiden väittämät identiteetit ja valtuuttamisella todennetut kohteet saavat identiteettiin sidotut oikeudet. Todentaminen edellyttää aina valtuustietoja, jotka voidaan varmistaa. Tähän tarkoitukseen soveltuvat esimerkiksi digitaaliset varmenteet, jotka hyödyntävät julkisen avaimen salausta pohjana tunnistautumiselle, koska vain salaisen avaimen haltija voi suorittaa tietyt toimet kuten julkisen salaamisen tai yksityisen salauksen purkamisen. Varsinainen todentaminen voidaan toteuttaa muun muassa OAuth-protokollalla. Se tarjoaa perinteisiä menetelmiä turvallisemman tavan valtuuttaa kolmansien osapuolien pääsy resursseihin käyttämällä erillistä valtuutuskerrosta ja käyttöoikeuslipukkeita omien valtuustietojensa jakamisen sijasta. Lopulta viimeinen tärkeä toiminto eli todennus- ja valtuutustietojen välitys eri osapuolten välillä, voidaan toteuttaa SAML-protokollalla. Se ei ota kantaa itse todennustapahtumaan, mutta pystyy kuvaamaan millä tavalla ja milloin kohde on todennettu sekä millaisia käyttöoikeuksia kohteelle on myönnetty. Näiden tietojen pohjalta kohdejärjestelmä voi luottaa kohteen identiteettiin ja myöntää sille tarvittavat oikeudet.

3.2 Federointi

Federointi tarkoittaa kahden tai useamman organisaation tai muun tahon välistä luottamussopimusta, jonka pohjalta ne voivat luottaa toistensa tarjoamaan todentamis- ja identiteettitietoon [12, s. 5]. Federoinnin osapuolet jakautuvat kolmeen rooliin: käyttäjiin, palveluntarjoajiin (engl. service provider, SP) ja identiteetintarjoajiin (engl. identity provider, IdP). Tunnistuslähteet hallinnoivat ja välittävät käyttäjäidentiteettejä sekä mahdollisesti myös myöntävät käyttäjätunnisteita. Palveluntarjoajat taas tarjoa-

vat käyttäjille palveluita perustuen tunnistuslähteiltä saamaansa varmistukseen käyttäjän identiteetistä. [13, s. 82]

Federointi voidaan toteuttaa teknisesti käyttämällä muun muassa luvussa 3.1 esiteltyjä SAML- tai OAuth-protokollia [14, s. 6,11]. Seuraavaksi esiteltävä esimerkki teknisestä toteutuksesta on tehty käyttämällä SAML-protokollaa, koska se on yleisimmin federointiin käytetty protokolla. Kun käyttäjä yrittää käyttää federoinnin piirissä olevaa palvelua, palveluntarjoaja muodostaa SAML-todentamispyynnön ja välittää sen käyttäjän identiteetintarjoajalle. Identiteetin tarjoaja vastaanottaa ja vahvistaa todentamispyynnön ja luo SAML-vakuutuksen, joka sisältää käyttäjän identiteetin tarvittavine identiteettiattribuutteineen. Tämän jälkeen identiteetintarjoaja allekirjoittaa sekä salaa digitaalisesti tehdyn vakuutuksen ja lähettää sen takaisin palveluntarjoajalle. Palveluntarjoaja vastaanottaa vakuutuksen ja vahvistettuaan sen aitouden purkaa sen salauksen ja jakaa vakuutuksen sisältämät identiteettiattribuutit palvelusovellukselle. Sovellus käyttää näitä tietoja käyttäjän sisäänkirjaamiseen ja palvelu on näin käyttäjän käytettävissä. [14, s. 6]



Kuva 5 Tupas-palvelun toimintamalli [16, s. 5, piirretty uudestaan]

Suomessa hyvä yleisesti tunnettu esimerkki federoidusta palvelusta on verkkopankkikirjautuminen johonkin VETUMA-palvelua [15] hyödyntävään palveluun Tupas-tunnistautumisen [16] kautta. Kuvassa 5 on esitetty Tupas-palvelun toiminnallinen malli, joka kuvaa yleisesti federoinnin vaiheet. Tupas-palvelun kautta tapahtuvan federoinnin eri vaiheet on selitetty lyhyesti alla:

1. Asiakas haluaa käyttää jonkin palveluntarjoajan asiointipalvelua [16, s. 5], esimerkiksi KELA:n sähköisen asioinnin palvelua.

2. Palveluntarjoaja lähettää asiakkaalle tunnistuspyynnön, jonka tiedot hän voi tarkastaa ennen eteenpäin lähettämistä. Tietojen muuttaminen ei kuitenkaan ole mahdollista. [16, s. 5]

3. Asiakas painaa oman pankkinsa painiketta, joka ohjaa hänet tunnistuspalveluun ja samalla tunnistuspyyntö tietoineen välittyy pankille [16. s. 5], joka toimii palvelussa identiteetintarjoajana.

4. Pankki (identiteetintarjoaja) lähettää asiakkaalle tunnistuspyynnön [16. s. 6].

5. Asiakas tunnistautuu pankkiinsa [16. s. 6] verkkopankkitunnuksilla.

6. Kun asiakas on tunnistautunut onnistuneesti, pankki muodostaa "Tupas-tunnisteen", joka asiakkaan pitää hyväksyä ennen kuin se lähetetään eteenpäin palveluntarjoajalle [16, s. 6].

7. Hyväksymisen jälkeen tunniste lähetetään palveluntarjoajalle [16, s. 6].

8. Palveluntarjoaja varmistaa Tupas-tunnisteen oikeellisuuden ja liittää tunnisteen asiakkaan palvelutapahtumaan [16, s. 6].

Viimeisen askeleen jälkeen käyttäjä on kirjautunut palveluun, esimerkiksi aiemmin mainittuun KELA:n sähköisen asioinnin palveluun. Palvelu käyttää vain identiteetintarjoajalta saamiaan identiteettitietoja, joten jos kirjautuminen tapahtuu vahingossa, tai tarkoituksella, toisen henkilön pankkitunnuksilla, KELA:n palvelussa käsitellään pankkitunnuksien haltijan henkilötietoja. Vaiheista voidaan huomata, että ne vastaavat pääpiirteittäin aiemmin esitettyä SAML-protokollaan perustuvaa federointiesimerkkiä ja VETUMA-palvelulla on myös tunnistautumista varten toteutettu SAML-protokollarajapinta [17, s. 3]. Tupas-esimerkki eroaa kuitenkin aiemmasta SAML-esimerkistä siinä, että tässä jälkimmäisessä tapauksessa identiteetintarjoaja ja palveluntarjoaja eivät ole suoraan yhteydessä toisiinsa vaan kaikki tiedot kulkevat asiakkaan selaimen kautta ja vaativat asiakkaan hyväksynnän.

OpenID

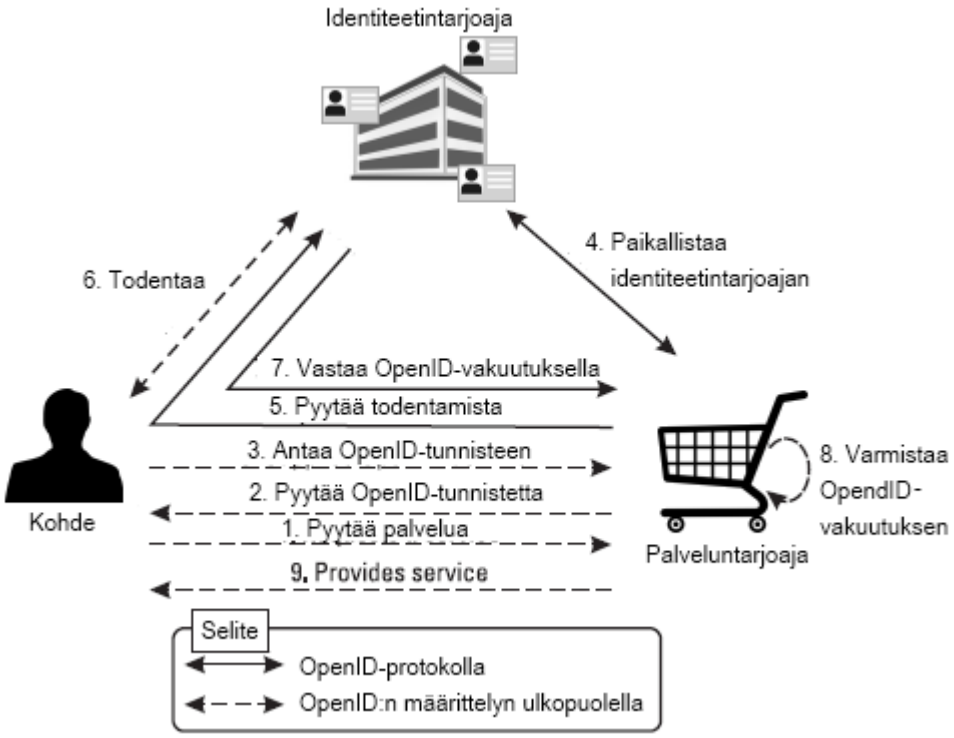
Edellisessä esimerkissä kerrottiin, esimerkiksi SAML-protokollaa voidaan käyttää federoinnin toteuttamisessa. Siihen voidaan kuitenkin käyttää myös eri lähtökohdista suunniteltuja standardeja kuten esimerkiksi OpenID-standardia [18].

OpenID mahdollistaa sen, että kohteet voivat valita dynaamisesti identiteetintarjoajiaan. OpenID esittää identiteetin Uniform Resource Indicator (URI) [19] -tyyppisenä merkkijonona, jota voidaan käyttää missä tahansa Internetissä. OpenID sisältää useita spesifikaatioita mukaan lukien OpenID Authentication, Attribute Exchange, Simple Registration Extension ja Provider Authentication Policy Exchange. Protokollamielessä OpenID on hyvin samankaltainen SAML 2.0:n WebSSO-profiilin kanssa. Molemmat käyttävät internetselaimen HTTP-protokollan uudelleenohjausmekanismia lähettääkseen todennustuloksia identiteetintarjoajien ja palveluntarjoajien välillä. Ne eroavat kuitenkin merkittävästi niissä mekanismeissa miten identiteetintarjoajat löydetään

sekä niiden tuottaman identiteettitransaktiotiedon ilmaisullisuudessa. OpenID antaa kohteiden valita identiteetintarjoajansa joka kerta, kun ne haluavat suorittaa identiteettitransaktion. SAML taas määrittelee vain sen formaatin, jolla identiteetintarjoajien sijaintitiedot kuvataan. [2, s. 98]

OpenID Authentication 2.0 määrittelee miten identiteetintarjoajat välittävät eteenpäin kohteen todentamisen tulokset palveluntarjoajille. Kohteet saavat pääsyn palveluntarjoajan palveluihin niillä identiteetintarjoajilta saaduilla todennustapahtumiin perustuvilla vakuutuksilla (engl. assertions). Vakuutuksia vaihdetaan palveluntarjoajien ja identiteetintarjoajien välillä HTTP-protokollan uudelleenohjauspyynnöillä kohteen selaimen kautta. Riippuen OpenID-ratkaisun toteutuksesta kohteet voivat joko lähettää globaalisti yksilöivät OpenID-tunnisteet URI-merkkijonona palvelintarjoajille tai valita identiteetintarjoajan jokaisella palveluntarjoajalla. [2, s. 98]

OpenID-standardissa kohteet voivat valita identiteetintarjoajan erikseen jokaiselle transaktiolle. Tätä varten OpenID 2.0 tarjoaa mekanismeja, joilla palveluntarjoajat voivat löytää kohteiden valitsemien identiteetintarjoajien sijainnit. Näitä sijaintien löytämismekanismeja on kolme: Extensible Resource Indicator (XRI) [20], Yadis-protokolla [21] sekä HTML-pohjainen löytäminen. Jos XRI-merkkijonoa käytetään kohteen identiteetin tunnisteena, niin identiteettiä hallinnoivan identiteetintarjoajan sijainti voidaan selvittää itse XRI-merkkijonosta. Jos taas kohteen identiteetin tunnisteena käytetään URI-merkkijonoa, pitäisi ensi kädessä käyttää Yadis-protokollaa identiteetintarjoajan sijainnin selvittämiseen. Siinä tapauksessa, että Yadis-protokolla ei löydä sijaintia, tulisi turvautua HTML-pohjaiseen löytämiseen. Tämä edellyttää, että identiteetin tunnisteena oleva URI-merkkijono sisältää identiteetintarjoajan sijainnin kertovat HTML-dokumentit. [2, s. 98–99]



Kuva 6. OpenID-standardin toimintamalli [2, kuva 4.12, piirretty uudestaan]

Kuva 6 havainnollistaa OpenID-standardin toimintaa. Vaiheet on selitetty alla:

1. Kohde lähettää palvelupyynnön palveluntarjoajalle. Palveluntarjoaja haluaa todentaa kohteen [2, s. 99–100].

2. Palveluntarjoaja pyytää OpenID-tunnistetta kohteelta [2, s. 99–100].

3. Kohde lähettää OpenID-tunnisteensa [2, s. 99–100].

4. Palveluntarjoaja paikallistaa identiteetintarjoajan kohteen lähettämän tunnisteen perusteella [2, s. 99–100].

5. Palveluntarjoaja pyytää todennustietoa identiteetintarjoajalta HTTP-uudelleenohjauksella kohteen käyttämän selaimen kautta [2, s. 99–100].

6. Identiteetintarjoaja ja kohde suorittavat todentamisen. Se, miten tämä todennus tapahtuu on OpenID-määrittelyn ulkopuolella. Identiteetintarjoaja todentaa kohteen onnistuneesti tämän antamalla käyttäjänimellä ja salasanalla. Todennus voi tapahtua myös muilla tavoin, kuten esimerkiksi digitaalisella varmenteella, mutta OpenID ei määrittele mitään mekanismia, jolla todennusmetodin voisi kommunikoida eteenpäin. Identiteetintarjoaja myöntää vakuutuksen, joka kuvaa todennuksen tapahtuneen onnistuneesti. [2, s. 99–100]

7. Identiteetintarjoaja lähettää todennusvakuutuksen palveluntarjoajalle HTTP-uudelleenohjausta käyttäen [2, s. 99–100].

8. Palveluntarjoaja vahvistaa saamansa todennusvakuutuksen [2, s. 99–100].

9. Palveluntarjoaja tarjoaa kohteelle tämän pyytämän palvelun. [2, s. 99–100]

Yhteenvetona federointi perustuu organisaatioiden tai tahojen välisille luottamussuhteelle, jossa eri tahot voivat luottaa toistensa tarjoamiin todentamis- ja identiteettitietoihin. Federointi toteutetaan useimmiten SAML-protokollalla, mutta siihen voidaan käyttää myös muun muassa OAuth-protokollaa tai OpenID-standardia. OpenID tarjoaa mahdollisuuden dynaamiseen identiteetintarjoajan valintaan eli kohde voi erikseen valita identiteetintarjoajansa jokaiseen identiteettitransaktioon. Federointi on houkutteleva valinta monille organisaatioille, koska helpottaa niiden taakkaa poistaen tarpeen pitää ajantasaista käyttäjärekisteriä kaikista oman organisaation ulkopuolisista vierailevista käyttäjistä. Jotkin organisaatiot voivat myös ulkoistaa koko todentamisen ulkoiselle osapuolelle ja säästää näin oman ratkaisun kehityskustannuksissa ja toteutusajassa.

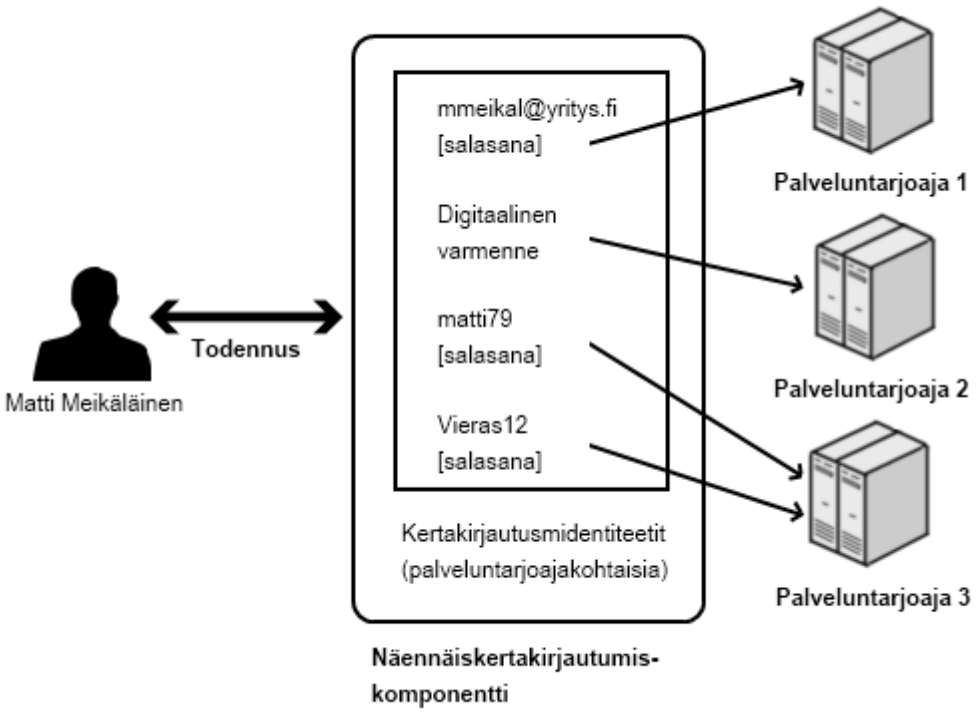
3.3 Kertakirjautuminen

Kertakirjautumien (engl. Single Sign-on, SSO) on yleistermi sellaiselle toteutukselle, jossa käyttäjä kirjautuu vain kerran istunnon (engl. session) aikana tai vain yhteen instanssiin, jonka jälkeen kaikki seuraavat tunnistautumiset muihin järjestelmiin ja resursseihin tapahtuvat automaattisesti [22, s. 270–271]. Kertakirjautumisen toteutustavat voidaan jakaa karkeasti näennäiskertakirjautumiseen ja (varsinaiseen) kertakirjautumiseen. Varsinainen kertakirjautuminen voidaan jakaa edelleen useampaan tyyppiin, joista yleisimmät ovat yrityskertakirjautuminen (engl. Enterprise Single Sign-on,

ESSO) ja verkkokertakirjautuminen (engl. Web-based Single Sign-on, WSSO) [2, s. 55]. Näitä kertakirjautumisen eri toteutustapoja ja tyyppejä esitellään seuraavaksi.

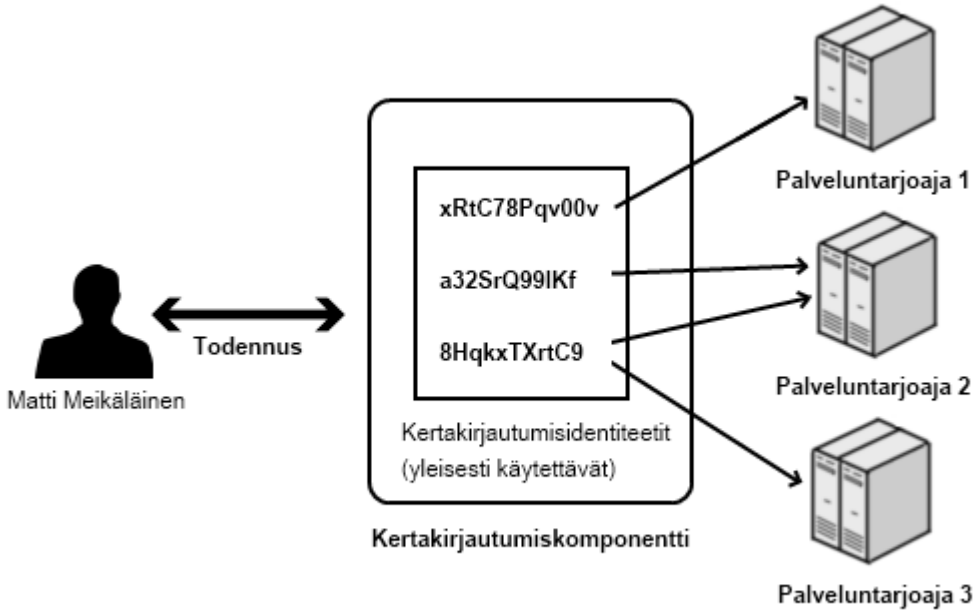
Näennäiskertakirjautuminen (engl. Pseudo Single Sign-On, Pseudo SSO) tarkoittaa sellaista toteutusta, jossa kertakirjautumiskomponentti kerää ja tallettaa kaikki käyttäjän valtuustiedot (engl. credentials), kuten vaikkapa käyttäjänimi-salasana-parit tai julkisen salauksen varmenteet, ja käyttää niitä käyttäjän puolesta automaattisesti. Istunnon alussa käyttäjä kirjautuu kerran kertakirjautumiskomponenttiin ja tämän jälkeen kertakirjautumiskomponentti hoitaa kaikki seuraavat kirjautumiset automaattisesti. Se valitsee ja syöttää palveluntarjoajakohtaiset käyttövaltuudet aivan samalla tavalla kuin käyttäjä tekisi manuaalisesti, esimerkiksi täyttämällä käyttäjänimen ja salasanan palveluntarjoajan kirjautumisikkunaan. [23, s. 382] Näennäiskertakirjautumista on havainnollistettu kuvassa 7.

Todellisessa kertakirjautumisessa kirjautuminen tapahtuu vain kerran Authentication Service Provider (ASP) -komponenttiin, ja tämän jälkeen todennustiedot välitetään vakuutusviesteillä kullekin kertakirjautumisen piirissä olevalle palvelulle tai järjestelmälle käyttötarpeen mukaan. Edellytyksenä kertakirjautumisen toiminnalle kuitenkin on, että ASP-komponentin ja palveluntarjoajien välillä on oltava ennalta muodostettu luottamussuhde, jotta palveluntarjoajat voisivat luottaa ASP-komponentin välittämiin vakuutuksiin. Tällaisessa kertakirjautumisen toteutuksissa käyttäjäidentiteettien ja palveluntarjoajien suhde on monen suhde moneen (n:m), joten yksi käyttäjäidentiteetti voi olla sidottu useampaan palveluntarjoajaan ja sama myös toisin päin (ks. Kuva 8). [24, s. 251]



Kuva 7: Esimerkki näennäiskertakirjautumisesta [24, s. 251, kuva 1]

Näennäiskertakirjautumisen ja kertakirjautumisen pohjimmainen ero tulee muun muassa siitä, että vaikka käyttäjä itse kirjautuukin näennäiskertakirjautumisessa vain kerran, kirjautuu kertakirjautumiskomponentti kuitenkin jokaiselle palveluntarjoajalle erikseen. Todellisessa kertakirjautumisessa on vain yksi kirjautumistapahtuma ASP-komponentille ja loppu hoidetaan vakuutuksien välityksellä. Näennäiskertakirjautumisessa kuvaus käyttäjän käyttäjäidentiteettien ja palveluntarjoajien välillä on rajoitetumpi kuin todellisessa kertakirjautumisessa, monen suhde yhteen (n:1). Tämä tarkoittaa, että jokainen käyttäjäidentiteetti voi olla sidottu vain yhteen palveluntarjoajaan, vaikka palveluntarjoajaan voikin olla sidottu useita käyttäjäidentiteettejä. [24, s. 250] Näennäiskertakirjautuminen ei myöskään edellytä minkäänlaista luottamussuhdetta kertakirjautumiskomponentin ja palveluntarjoajien välillä toisin kuin todellinen kertakirjautuminen. [24, s. 251]



Kuva 8 Esimerkki kertakirjautumisesta [24, s. 251, kuva 2]

Kertakirjautumisen yleisimmät muodot

Yrityskertakirjautuminen on nimensä mukaisesti saman yrityksen tai organisaation sisäisiin järjestelmiin tapahtuvaa kertakirjautumista [10, s. 135]. Koska eri järjestelmät ja sovellukset voivat käyttää omia ei-standardoituja metodeja kirjautumiseen [2, s. 55], joudutaan jokaisella tällaiselle järjestelmälle tekemään omat liittimet tai agentit, jotka tulkkaavat kertakirjautumiseen käytettävät valtuustiedot järjestelmän ymmärtämään muotoon [25, s. 4]. Käyttöjärjestelmäkertakirjautuminen ja federoitu kertakirjautuminen ovat yrityskertakirjautumisen alaluokkia.

Käyttöjärjestemäkertakirjautuminen tarkoittaa esimerkiksi Windows-käyttöjärjestelmien mahdollisuutta käyttää käyttöjärjestelmän kirjautumistietoja edelleen sovelluksiin kirjautumiseen. Windows-käyttöjärjestelmässä tämä kertakirjautumistapa rajoittuu vain niihin sovelluksiin, jotka käyttävät kirjautumiseen SSPI-ohjelmointirajapin-

taa. Myös UNIX-pohjaisissa käyttöjärjestelmissä samankaltainen kirjautumistietojen välitys voidaan saavuttaa GSSAPI-ohjelmistorajapinnan avulla. [26]

Federoitu kertakirjautuminen perustuu nimensä mukaisesti federointiin eli käyttäjät tunnistautuvat ensin luotetulle tunnistuslähteelle, joka sitten hoitaa loput kirjautumisen kohdejärjestelmiin. Yrityskäytössä esimerkiksi Kerberos-protokolla [27] ja Active Directory Federation Service -palvelu [28] ovat yleisiä ratkaisuja federoidun kertakirjautumisen toteuttamiseksi.

Verkkokertakirjautuminen tarkoittaa verkkopalveluihin kirjautumista internetselaimella [10, s. 135]. Yhä useampia sovelluksia käytetään selaimella internetin yli, joten verkkokertakirjautumisella on tärkeä rooli, vaikka se onkin rajoittunut vain verkkopalvelimilla toimiviin sovelluksiin. Tämä tarkoittaa, ettei verkkokertakirjautumisella voi sellaisenaan kirjautua ei-verkkopohjaisiin sovelluksiin kuten esimerkiksi asiakas-palvelin-sovelluksiin. [25, s. 3] Microsoft Passport toimii esimerkkinä verkkokertakirjautumisesta [26].

Yhteenvetona kertakirjautuminen mahdollistaa käyttäjän kirjautumisen useisiin kohdejärjestelmiin tai -sovelluksiin kirjautumalla vain kerran ja yhdellä salasanalla. Tämä säästää käyttäjien aikaa ja kognitiivista taakkaa lukuisten eri salasanojen muistamisesta ja kirjoittamisesta. Kertakirjautuminen jakautuu karkeasti näennäiskertakirjautumiseen ja todelliseen kertakirjautumiseen. Kategorioiden erona on se, että näennäiskertakirjautumisessa kertakirjautumiskomponentti kuitenkin joutuu kirjautumaan jokaiseen kohdejärjestelmään erikseen niiden omilla salasanoilla siinä missä todellisessa kertakirjautumisessa kertakirjautumiskomponentti käyttää vakuutuksia kohdejärjestelmiin kirjautumiseen. Kertakirjautumisen yleisimmät tyypit ovat korkealla tasolla yrityskertakirjautuminen ja verkkokertakirjautuminen. Ne eivät ole varsinaisesti kilpailevassa asemassa keskenään, vaan ne täydentävät toisiaan. Yrityskertakirjautuminen voi liittää monimuotoisempia järjestelmiä ja sovelluksia piiriinsä kuin verkkokertakirjautuminen, mutta toisaalta se on rajattu yrityksen sisäisiin järjestelmiin. Verkkokertakirjautuminen taas on rajattu verkkopalveluihin, mutta mahdollistaa kirjautumisen ulkopuolisten tahojen tarjoamiin sovelluksiín julkisen verkon kuten Internetin yli. Matalammalla tasolla yrityskertakirjautuminen voidaan vielä toteuttaa eri tavoin, esimerkiksi federoinnin avulla tai käyttöjärjestelmän kirjautumistietoja välittämällä.

3.4 Provisiointi

Provisioinnin periaatteita ja toimintaa käsiteltiin jo aikaisemmin luvussa 2.3.2, joten tämä luku keskittyy provisiointiprotokollien esittelyyn ja vertailuun. Ensin esitellään vanhempi Service Provisioning Markup Language (SPML) ja sen jälkeen tuoreempi System for Cross-domain Identity Management (SCIM) -protokolla.

Service Provisioning Markup Language (SPML)

Service Provisioning Markup Language (SPML) 2.0 [29] on OASIS-organisaation kehittämä provisiointiin tarkoitettu protokollastandardi. Se sisältää standardit käyttäjätilien provisioinnille, deprovisioinnille, kyselyille (engl. querying), muokkaamiselle, väliaikaiselle käytön keskeyttämiselle (engl. suspending) ja palauttamiselle erilaisten järjestelmien, laitteiden ja ei-digitaalisten resurssien välillä. Protokolla perustuu XML-pohjaiseen raamiin, joka mahdollistaa provisiointijärjestelmän toiminnallisuuksien skaalaamisen kaikkiin sitä tukeviin järjestelmiin ja palveluihin aina yritysjärjes-

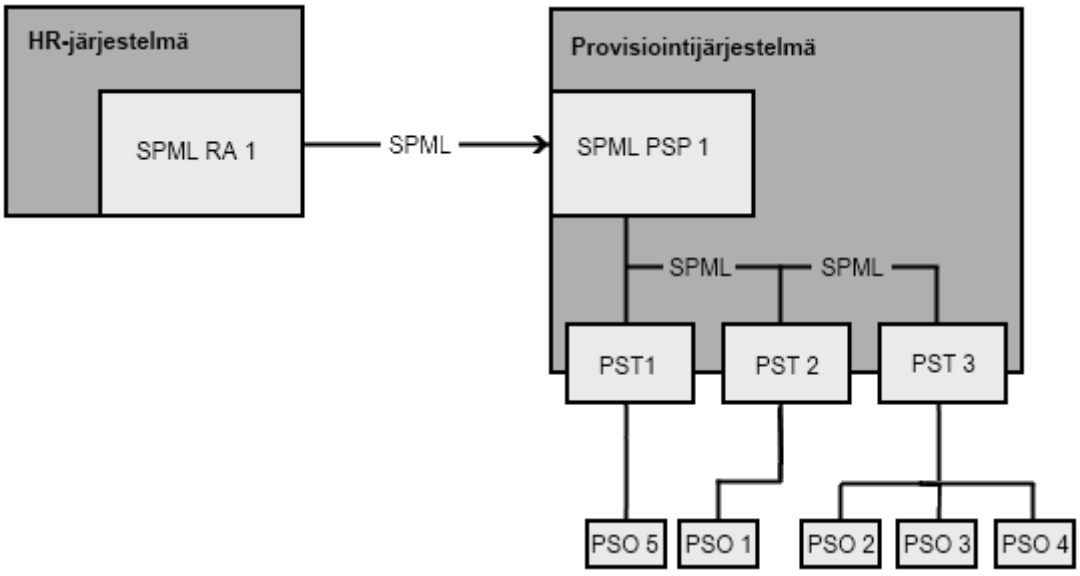
telmistä verkkopalveluihin. Se tarjoaa palveluja tarjoaville yrityksille yhteisen kielen, jolla ne voivat turvallisesti hallita käyttäjäidentiteettejä ja kohdentaa niihin sidottuja resursseja. [30, s. 93–94]

SPML-protokollan toimintamalli perustuu kolmelle roolille: Requesting Authority (RA), Provisioining Service Provider (PSP) ja Provisioning Service Target (PST).

- *Requesting Authority* on sovelluskomponentti, joka lähettää SPML-pyyntöjä provisointipalvelua tarjoavalla Provisioning Service Provider -komponentille. Jokainen komponentti, joka lähettää SPML-viestejä toimii siis lähettäessään RA-komponentin roolissa. Tämä edellyttää, että RA-komponentin ja PSP-komponentin välillä on oltava luottamussuhde. SPML-standardi ei kuitenkaan ota kantaa siihen miten tämä luottamussuhde muodostetaan. [29, s. 10– 11]

- *Provisioning Service Provider* -komponentti kuuntelee ja prosessoi SPML-pyyntöjä sekä palauttaa niiden tulokset. Jokainen komponentti, joka vastaanottaa ja prosessoi SPML-pyyntöjä, kuten esimerkiksi identiteetinhallintajärjestelmä, toimii sillä hetkellä PSP-komponentin roolissa. RA-komponentin kuvauksessa mainittu luottamussuhde on molemminpuolinen ja pätee myös PSP-komponenttiin. [29, s. 11]

- *Provisioning Service Target* edustaa sellaista määränpäätä tai loppukohdetta (engl. endpoint), jolle PSP-komponentti voi suorittaa provisiointitoimia, kuten esimerkiksi tilien luomista tai muokkaamista. [29, s. 11] Näitä provisiointitoimien kohteita kutsutaan nimellä Provisioning Service Object (PSO). PSO-objektit sisältävät identiteettien attribuutit. [5 s. 9] PST voi myös toimia PSP-komponentin roolissa [31 s. 9].



Kuva 9. SPML-roolien keskinäiset suhteet ja viestien kulku [5, kuva 1][31, s. 11, piirretty uudestaan]

SPML:n eri roolien keskinäisiä suhteita ja viestiketjuja on kuvattu kuvassa 9. Kuvassa HR-järjestelmän RA 1 -komponentti lähettää SPML-pyynnön PSP 1 -komponentille,

joka vastaanottaa pyynnöt ja suorittaa niiden pohjalta provisiointitoimia eri PST-kohteiden sisältämille PSO-objekteille. Kaikkien komponenttien välinen viestintä tapahtuu SPML-protokollalla.

SPML 2.0 –standardi sisältää seuraavat viisi perusoperaatiota:

- *ListTargets*-toiminto listaa kaikki PSP-komponentin tarjoamat PST-kohteet [5, s. 9].
- *Add*-toiminto lisää uuden PSO-objektin PST-kohteeseen [5, s. 9].
- *Modify*-toiminto muokkaa olemassa olevan PSO-objektin attribuutteja PST-kohteen sisällä [5, s. 9].
- *Delete*-toiminto poistaa PSO-objektin PST-kohteesta [5, s. 9].
- *Lookup*-toiminto etsii PSO-objektia annetulla PSO-tunnisteella [5, s. 9].

Yllä listatuilla toiminnoilla voi jo suorittaa pääasialliset provisioinnissa tarvittavat tehtävät. Identiteetit voidaan luoda Add-toiminnolla, niitä voidaan hakea Lookup-toiminolla ja tietojen muuttuessa niitä voidaan muokata Modify-toiminnolla. Lopuksi, elinkaartensa päättyessä, identiteetit voidaan poistaa Delete-toiminnolla. SPML-protokolla tarjoaa siis kaikki provisiointiin tarvittavat perustoiminnallisuudet, mutta se ei ole saavuttanut suurta suosiota [32]. Tämän havainnon pohjalta on alettu kehittää pilviystävällisempää protokollaa, jota käsitellään tässä luvussa seuraavaksi.

System for Cross-domain Identity Management (SCIM)

System for Cross-domain Identity Management (SCIM) [33] on Representational State Transfer (REST) [34, luku 6] -tyyppinen sovelluskerroksen protokolla, joka on suunniteltu varsinkin pilvipalveluissa tapahtuvaa identiteetinhallintaa silmällä pitäen. REST-arkkitehtuurityyli kuvaa sitä miten Internetin kuuluisi toimia ja sitä on käytetty muun muassa HTTP- ja HTML-standardien määrittelyssä [34, s. 107–108]. SCIM-protokollan tarkoitus on vähentää identiteetinhallinnan operaatioiden monimutkaisuutta ja kustannuksia tarjoamalla yhteisen käyttäjäskeemamallin, jota voidaan käyttää standardoiduilla protokollilla. Yksi sen kantavista ajatuksista onkin voida käyttää olemassa olevia todennus-, valtuutus- ja yksityisyysmalleja, mutta yksinkertaistaa kehittämistä ja integrointia. [33, s. 1]

SCIM-protokolla sisältää kahdeksan yksinkertaista operaatiota, joilla saadaan katettua kuitenkin monia identiteetinhallinnan perustarpeista [35]. Operaatiot pohjautuvat REST-ohjelmointirajapintaan, joka käyttää tunnettuja HTTP-protokollan metodeja GET, POST, PUT, DELETE ja PATCH [33, s. 4]. SCIM-protokollan operaatiot on listattu alla esimerkkeineen.

- Create-operaatio – uuden resurssin luominen (esim. POST https://example.com/{v}/{resource}) [35][33, s. 4]
- Read-operaatio – ennestään luodun resurssin lukeminen (esim. GET https://example.com/{v}/{resource}/{id}) [35][33, s. 4]

- Replace-operaatio – korvaa resurssin täysin (esim. PUT https://example.com/{v}/{resource}/{id}) [35][33, s. 4]

- Delete-operaatio – poistaa resurssin (esim. DELETE https://example.com/{v}/{resource}/{id}) [35][33, s. 4]

- Update-operaatio – päivittää resurssin (esim. PATCH https://example.com/{v}/{resource}/{id}) [35][33, s. 4]

- Search-operaatio – hakee resurssin tai resurssin osan (esim. GET https://example.com/{v}/{resource}?filter={attribute}{op}{value}&sortBy={attributeName}&sortOrder={ascending|descending}) [35][33, s. 4]

- Bulk-operaatio – muokkaa useaa resurssia kerralla (esim. POST https://example.com/{v}/Bulk) [35][33, s. 4]

SCIM-protokollan perusoperaatioita tarkastellessa voi huomata, että ne muistuttavat paljon SPML-protokollan perusoperaatioita - Add ja Create, Modify ja Update, Lookup ja Search sekä yhteinen Delete. Samankaltaisista perustoiminnallisuuksista huolimatta protokollilla on selkeitä eroja, joita käsitellään seuraavaksi.

SPML- ja SCIM-protokollien vertailua

SPML- ja SCIM-protokollan erot eivät perustu pääasiallisesti niiden funktionaalisiin toiminnallisuuksiin – molemmat pystyvät suorittamaan provisioinnissa tarvittavat tehtävät – vaan niiden arkkitehtuuriratkaisuihin. Etenkin pilvipalvelunäkökulmasta näillä arkkitehtuuriratkaisuilla vaikuttaa kuitenkin olevan suuri merkitys. Kyse ei ole ensisijaisesti siitä, että pilvipalvelujen vaatimukset provisioinnille olisivat perustavasti erilaiset, vaan siitä, että pilvipalveluissa ei voida käyttää sellaisia oikoteitä, joita perinteisissä provisiointijärjestelmissä on voitu tehdä. Provisiointijärjestelmien valmistajat eivät ole puskeneet SPML-protokollaa vahvasti yrityssovellusten valmistajille, koska perinteisissä järjestelmissä on voitu aina luoda identiteettejä suoraan tietokantaan, eikä standardoidulle SPML-protokollalle ole ollut pakottavaa tarvetta. Pilvipalvelussa ei kuitenkaan tällaista oikotietä voida käyttää, joten standardoitu provisiointiohjelmointirajapinta tarvitaan. [32]

Pilvipalvelujentarjoajat eivät tarttuneet provisiointitarpeessaan valmiiseen SPML-standardiin, koska se on XML-pohjainen, minkä pilvipalvelujen tarjoajat kokivat monimutkaiseksi ja raskaaksi käyttää. Sen sijaan pilvipalveluntarjoajat, esimerkiksi Salesforce.com ja Google, loivat omat, yksityiset, REST- ja SOAP-pohjaiset ohjelmointirajapintansa. [32] SPML ei ollut siis ollut saanut tarpeeksi vakaata markkinapohjaa entuudestaan, eikä sitä pidetty riittävän helppona ja yksinkertaisena vaihtoehtona itse tehdyille ratkaisuille. SCIM-protokolla, jota lähdettiin kehittämään pilvipalvelujentarjoajien tarpeet mielessä, on yksinkertaisempi ja pohjautuu REST-arkkitehtuuriin, jota monet pilvipalvelut jo entuudestaan käyttävät [32]

Yhteenvetona sekä SPML- että SCIM-protokollat pystyvät suorittamaan kaikki identiteetinhallinnan perustoiminnot eli uomaan, hakemaan, päivittämään ja poistamaan identiteettejä. Kuitenkin erilaisista suunnitteluparadigmoista lähtöisin oleva yksinkertaisuus ja REST-arkkitehtuuripohja ovat luoneet SCIM-protokollalle SPML-protokol-

laa paremman kilpailuaseman pilvipalvelujen osalta. Tämän suosion karttumisen ja yleistymisen myötä SCIM-protokolla saattaa hyvin syrjäyttää SPML-protokollan muissakin sovelluskohteissa kuin pilvipalveluissa, koska SPML-protokollalla ei niissäkään ole perinteisesti ollut kovin vahvaa asemaa.

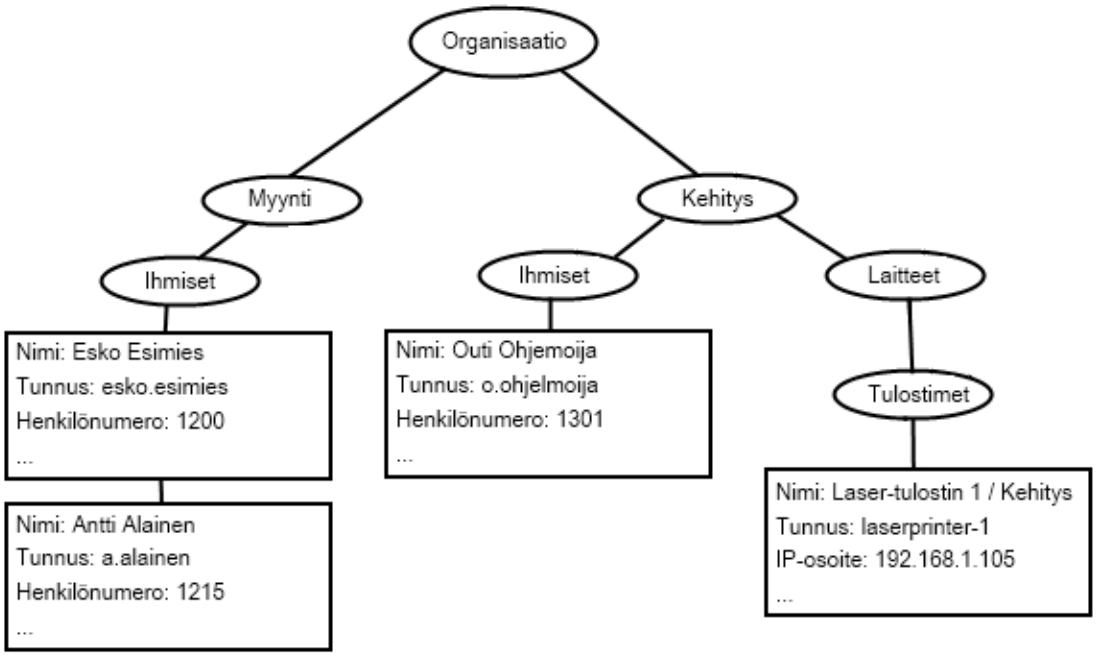
3.5 Hakemistopalvelut

Hakemistot ovat erikoistuneita tietokantoja, jotka on suunniteltu nopeita hakuoperaatioita varten. [36, s. 12][3, s. 78]. Ne koostuvat tyypillisesti jotain tiettyä rakennetta noudattavista tietueista, jotka sisältävät kuvaavaa tietoa kohteista, esimerkiksi ihmisistä tai laitteista. Nämä tietueet on yleensä jäsennelty hakemistossa hierarkkiseen puutyyppiseen rakenteeseen, mikä tekee tietueiden ryhmittelystä helppoa ja hakuoperaatioista nopeita. [37] Hakemistolla viitataan tässä kokonaiseen hakemistopalveluun, joka käsittää kaikki sovellukset, prosessit, politiikat ja laitteiston, joiden kautta hakemiston sisältö saatetaan saataville.

Hakemistojen ja niiden sisältämien tietueiden rakenteen ratkaisee hakemiston skeema. Se määrittelee mitä kenttiä ja attribuutteja tietueilla on, missä muodossa ne esitetään ja mitkä niistä ovat vapaaehtoisia ja mitkä taas pakollisia. [3, s. 78] Esimerkiksi sekä ihmis- että laitetietueilta voidaan molemmilta edellyttää, että niillä on oltava osastokenttä tiedoissaan, mutta esimieskenttää puolestaan ei välttämättä edellytettäisi laitteelta. Itse hakemiston puumaista tietorakennetta on havainnollistettu kuvassa 10. Kuvan esimerkissä on organisaatio, jonka alla on organisaatioon kuuluvat kaksi osastoa: myynti ja kehitys. Myynti-osastohaaran alla on vain ihmisidentiteettejä, ja ne on järjestetty hierarkkisesti esimiessuhteiden mukaisesti. Kehitys-osastohaaran alla on puolestaan sekä laite- että ihmisidentiteettejä. Kuvasta voi nähdä myös skeeman vastaavuudet ja eroavuudet ihmis- ja laiteidentiteettien välillä. Kaikilla tietueilla on nimi ja tunnus, mutta vain ihmisidentiteeteillä on henkilönumero ja esimerkin tulostimella taas IP-osoite. Esimerkissä esitetty rakenne ei kuitenkaan ole ainoa tapa kuvata organisaation rakennetta, vaan esimerkiksi jakautuminen ihmis- ja laiteidentiteetteihin saattaisi yhtä hyvin olla korkeammalla ennen osastoja, jolloin osastot olisivat niiden alahaaroja. Sopivin rakenne ja skeema riippuvat aina kunkin organisaation rakenteesta ja tarpeista.

Hakemistot on suunniteltu suurelle määrälle pieniä tietueita ja ne on optimoitu luku- tai hakuoperaatioita varten. Ne voivat sisältää jopa miljoonia tietueita, jotka ovat silti nopeasti haettavissa. Tämä tekee hakemistoista erittäin soveltuvia identiteettien varastoimiseen ja hakemiseen, ja hakemistot ovatkin useimmiten kriittinen osa identiteetinhallintajärjestelmien infrastruktuuria. [3, s. 78]

Useat organisaatiot tarvitsevat useita hakemistoja tallentaakseen kaikki identiteettitietonsa. Tietojen pitäminen vastaavina ja ajantasaisina sekä identiteettitietojen keskinäisten suhteiden säilyttäminen usean eri hakemiston välillä on kuitenkin haastavaa. Näitä ongelmia voidaan helpottaa aggregoimalla (engl. aggregating) identiteettitietoa eli keräämällä eri identiteettitietoja eri hakemistoista ja luomalla yhtenäisen kuvan niistä. Yhtenäisen kuvan aikaansaamiseksi voidaan käyttää muun muassa metahakemistoja (engl. metadirectories) tai virtuaalihakemistoja (engl. virtual directories). [3, s. 84]



Kuva 10: Esimerkki hakemiston rakenteesta ja tietueista [36, kuva 2.11 ja kuva 2.7, piirretty uudestaan]

Metahakemistot

Metahakemistot ovat kokoelmia erilaisista hakemistoista kerättyä ja yhdisteltyä hakemistotietoa, jotka muodostavat yhtenäisen näkymän useiden eri hakemistojen tiedoista. Tämän takia metahakemistosta voidaankin tehdä hakuja ikään kuin se olisi yksi hakemisto, joka sisältää kaikkien muiden varsinaisten hakemistojen tiedot. Nämä hakemistotiedot kerätään hakemistoista ja yhdistellään yleensä sovellusagenttien (engl. software agents) toimesta. Koska metahakemisto on abstraktio varsinaisista hakemistoista, itse hakemistoja voidaan muokata tai jopa vaihtaa eri valmistajan tuotteisiin ilman, että se näkyy mitenkään metahakemistosta hakuja tekeville sovelluksille. Muita metahakemistojen hyötyjä ovat helpotettu hallinto, koska kaikkiin hakemistoihin pääsee käsiksi yhden pisteen kautta, ja mahdollisuus poistaa eri hakemistojen redundantit tiedot tarpeettomina. [3, s. 85]

Metahakemistoihin toteuttamiseen liittyy kuitenkin teknillisiä ja hallinnollisia haasteita. Hallinnolliset haasteet ovat suurempia näistä kahdesta. Ne muodostuvat muun muassa tiedon omistajuuden, käytettävien tietoformaattien, nimiavaruuden, skeemojen ja lakivaatimusten määrittelystä sekä tietoturvallisuuden suunnittelusta. Teknilliset haasteet ovat hallinnollisia haasteita suoraviivaisempia ja koskevat pääasiassa metahakemiston yleistä arkkitehtuuria, nimiavaruuden yhtenäisyyttä, protokollia sekä datan synkronointia. [3, s. 85]

Virtuaalihakemistot

Virtuaalihakemistot ovat periaatteessa samankaltaisia kuin metahakemistot eli ne luovat yhtenäisen hakemistonäkymän useista eri hakemistoista. Ne kuitenkin toteuttavat tämän yhtenäistetyn näkymän eri tavalla. Siinä missä metahakemistot käyttävät agentteja tietojen keräämiseen ja synkronointiin, virtuaalihakemistot luovat yhtenäisen

näkymän hakemistoista käyttämällä reaaliaikaisia hakuja. Nämä haut perustuvat kuvauksiin virtuaalisen skeeman tietuekentistä hakemistojen todellisten skeemojen kenttiin. [3, s. 87]

Virtuaalihakemistojen toimintaperiaatteen erot metahakemistoihin poistavat myös joitain metahakemistoihin liittyviä haasteita. Virtuaalihakemistoilla ei esimerkiksi ole omaa tietovarastoa, vaan ne muuttavat yksittäisen virtuaalihakemistoon tehdyn haun useiksi hauiksi todellisiin hakemistoihin ja yhdistelevät palautetut hakutulokset reaaliaikaisesti käyttäjälle annettavaksi vastaukseksi. Tietovaraston puuttuminen poistaa tiedon synkronointiin liittyviä ongelmia, joita metahakemistoissa on. [3, s. 87]

Pohjimmiltaan virtuaalihakemistot tarjoavat rajapinnan hakemistoissa olevaan identiteettitietoon, jossa kaikki haut ja päivitykset tapahtuvat tosiaikaisesti. Tämä tekee virtuaalihakemistoista hyödyllisiä tilanteissa, joissa identiteettitiedot muuttuvat tiuhaan ja tosiaikaisuus on tärkeää. Rajapinnan virtuaalihakemiston ja todellisten hakemistojen välillä voi toteuttaa millä tahansa sopivalla protokollalla, mutta useimmiten tällainen rajanpinta on toteutettu LDAP-protokollalla. [3, s. 87]

LDAP

Lightweight Directory Access Protocol (LDAP) [38] on kevyt verkkopohjainen hakemistonhallintaprotokolla, joka perustuu vanhaan hierarkkiseen X.500-hakemistostandardiin[39]. X.500-hakemistostandardi määrittelee hajautetun ja hierarkkisen hakemistopalvelun, joka toimii yhteisellä nimiavaruudella ja jonka tarjoama palvelu on suunniteltu hyvin skaalautuvaksi ja laajennettavaksi. [3, s. 83] LDAP-protokolla on ikään kuin kevennetty versio X.500-standardista, ja siitä on karsittu paljon vanhemman standardin harvoin käytettyjä ominaisuuksia [40, s. 7]. LDAP-protokolla sisältää nykyisessä kolmannessa versiossaan vain yhdeksän protokollaoperaatiota, jotka esitelty alla kategorioittain:

- Kyselyoperaatiot: *search, compare.* Näillä operaatioilla voidaan tehdä kyselyjä ja vertailuja hakemistosta. [36, s. 56]

- Päivitysoperaatiot**:** *add, delete, modify, modify DN (rename).* Nämä operaatiot mahdollistavat hakemiston tietojen lisäämisen, poistamisen, päivittämisen ja muokkaamisen. [36, s. 56]

- Todentamis- ja kontrollioperaatiot: *bind, unbind, abandon*. Bind-operaatiolla asiakaskone (engl. client) voi tunnistautua istunnonmuodostusta varten syöttämällä oikean identiteettitunnisteen ja valtuustiedon. Unbind-operaatiolla asiakaskone voi taas lopettaa nykyisen session. Abandon-operaatiota käyttäen asiakaskone voi ilmoittaa hakemistopalvelimelle, ettei ole enää kiinnostunut aiemmin aloittamansa operaation tuloksista. [36, s. 56]

LDAP-protokollaa käyttävässä hakemistossa tietueisiin viitataan Distinguished Name (DN) –nimellä, joka muodostuu käänteisesti niistä haaroista, joiden läpi on kuljettava tietueeseen päästäkseen. DN-nimen alussa oleva vasemmanpuoleisin tunniste on nimeltään Relative Distinguished Name (RDN) ja sen oltava aina yksilöllinen saman haaran alla oleville tietueteille ja haaroille, jottei kahdelle tietueelle voisi tulla samaa DN-nimeä. [36, s. 74] Käyttäen kuvan 10 esimerkkiä pohjana Outi Ohjelmoijan DN-nimi voisi olla esimerkiksi

uid=o.ohjelmoija,ou=kehitys,dc=organisaatio

ja vastaavasti Lasertulostin-1:n DN-nimi taas olisi

uid=laserprinter-1,ou=tulostimet,ou=laitteet,ou=kehitys,dc=organisaatio.

Esimerkissä uid tarkoittaa käyttäjätunnusta (engl. user id), ou organisaatioyksikkö (engl. organization unit) ja dc toimialuekomponenttia (engl. domain component).

Yhteenvetona hakemistopalvelut ovat tärkeä identiteetin- ja pääsynhallinnan elementti, joiden kautta kaikki identiteettitiedot tallennetaan ja haetaan. Hakemistopalvelu koostuu hakemistoista, joissa varsinainen tieto on tallennettu hierarkkisiin puumaisiin tietokantoihin, sekä kaikesta laitteistosta ja infrastruktuurista, jota näiden hakemistojen pyörittämiseen vaaditaan. Useat organisaatiot joutuvat tallentamaan tietojaan useaan erilliseen hakemistoon, mikä voi aiheuttaa ongelmia tietojen yhtenevyyden ja ajantasaisuuden säilyttämiseen näiden eri hakemistojen välillä. Tämän ongelman mitigoimiseksi voidaan käyttää perinteisten hakemistojen lisäksi meta- tai virtuaalihakemistoja. Ne luovat aggregoidun yhtenäisen näkymän eri hakemistoista kerättyyn tietoon. Metahakemistot toteuttavat tämän fyysisesti ja virtuaalihakemistot loogisesti. Tämän vuoksi virtuaalihakemistot kärsivät yleensä vähemmistä ongelmista liittyen muun muassa tiedon synkronointiin ja tietoformaatteihin kuin metahakemistot. Käyttäjä- ja pääsynhallinnan sovellukset voivat käyttävät usein LDAP-protokollaa hakemistojensa hallintaan. Se on kevyt hakemistonhallintaprotokolla, joka sisältää vain yhdeksän perustoimintoa, jotka jakautuvat kysely-, muokkaus- ja todentamis- sekä kontrollioperaatioihin.

3.6 Identiteettien hallinnointi

Identiteeteille suoritettavia toimia, kuten esimerkiksi luontia, muokkaamista sekä oikeuksien myöntämistä, pitää hallita erilaisilla poliitikoilla koko identiteetin elämänkaaren ajan. Identiteettien hallinnointia käsitellään laajemmin luvussa 2.3.6 ja tämä luku keskittyy sen sijaan siihen käytettäviin standardeihin. OASIS-organisaation eXensible Access Control Markup Language (XACML) [41] on yksi näistä standardeista.

eXensible Access Control Markup Language (XACML)

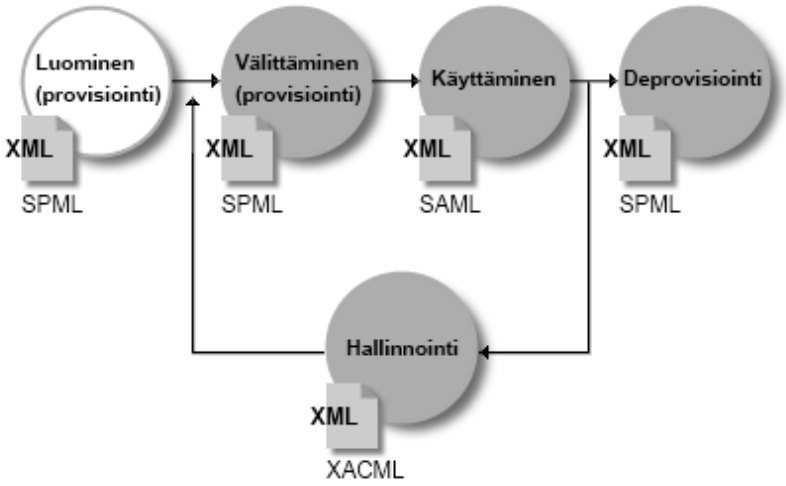
eXensible Access Control Markup Language (XACML) on XML-pohjainen kieli, jota käytetään pääsynhallintapolitiikoiden tallentamiseen ja jakamiseen. Sen ohjelmointikielinen luonne mahdollistaa hyvin hienojakoisten pääsynhallintasääntöjen luomisen. [3 s. 111] Säännöt voivat perustua muun muassa:

- Pyyntöä tekevän kohteen identiteettiattribuuteille – pääsy johonkin resurssiin voidaan esimerkiksi rajoittaa vain sellaisille kohteille, jotka työskentelevät kirjanpidossa [3 s. 111].
- Toimelle, joka aiotaan suorittaa – esimerkiksi aiotaanko dokumenttia lukea vai muokata [3 s. 111].
- Kellonaikaan, kuten toimistoaikoihin tai työvuoroihin [3 s. 111].

- Käytetylle todennusmekanismille – joitain resursseja saattaa esimerkiksi voida käyttää ainoastaan toimikorttitodennuksen kautta [3 s. 111].

- Käytetylle protokollalle. Pääsy resurssiin voi olla sallittu esimerkiksi salattua HTTPS-protokollaa käyttäville yhteyksille, mutta ei tavallista HTTP-protokollaa käyttäville yhteyksille. [3 s. 111]

Yhdistelemällä tällaisia sääntöjä sopivalla tavalla voidaan identiteettien käyttöä hallita hyvin monipuolisesti ja erilaisten organisaatioiden tarpeisiin mukautuvasti.



Kuva 11. SPML-, SAML- ja XACML-protokollien yhteistoiminta [3, kuva 11.1, piirretty uudestaan]

Yhdessä kahden tässä luvussa aiemmin mainitun XML-pohjaisen protokollan, SPML- ja SAML-protokollan, kanssa XACML luo yksinkertaisen kokonaisuuden, jolla toteuttaa identiteetin elinkaaren kaikki luvussa 2.3 esitetyt vaiheet. Kuva 11 auttaa havainnollistamaan tätä yhteistoimintaa. SPML-protokollalla voidaan ensin provisioida identiteetti ja sitten välittää se kohdejärjestelmille. Identiteetin käytössä tapahtuvat todennuksien ja valtuutuksien välittäminen järjestelmien ja eri toimialueiden välillä voidaan taas toteuttaa SAML-protokollalla. Näiden vaiheiden aikana XACML-protokolla mahdollistaa identiteettien käyttöä koskevien politiikoiden hallinnoinnin ja lopulta elinkaaren päättyessä SPML-protokollaa voidaan käyttää identiteetin deprovisioimiseen.

3.7 Yhteenveto

Todentaminen ja valtuuttaminen ovat pääsynhallinnan keskeisimpiä toimintoja. Ne varmistavat kohteen oikeuden käyttämäänsä identiteettiin ja siihen sidottuihin oikeuksiin. Todentamisella varmistetaan, että kohde on käyttämänsä identiteetin oikeutettu haltija. Tähän käytetään jonkinlaista valtuustietoa, kuten X.509-standardin mukaista digitaalista varmennetta, jossa kohteen identiteettiattribuutit on sidottu sen julkiseen salausavaimeen. Tällöin tätä julkista avainta vastaavan yksityisen avaimen haltija voi todistaa oikeutensa kyseiseen identiteettiin. Valtuuttamisella tarkoitetaan oikeuksien myöntämistä kohteelle todennuksessa varmistettuun identiteettiin perustuen. Tämä

toteutetaan myös valtuustiedoilla, esimerkiksi aiemmin mainituilla varmenteilla. Näitä valtuustietoja voidaan tarvittaessa myös delegoida eteenpäin, jolloin yksi identiteetti saa lisäksi toisen identiteetin oikeudet ja voi toimia toisen identiteetin puolesta. Todennuksessa ja valtuuttamisessa yleisesti käytettäviä standardeja ovat muun muassa SAML ja OAuth. SAML on hyvin laajalti käytetty todennus- ja valtuustietojen välitysprotokolla, joka ei ota kantaa itse todentamistapaan, vaan keskittyy pelkästään todennus- ja valtuustietojen välittämiseen. OAuth on todentamisprotokolla, joka tarjoaa perinteisestä todennuksen asiakas-palvelin-mallista poiketen erillisen valtuutuskerroksen, joka mahdollistaa asiakaskoneiden ja resurssien omistajan roolien erottamisen toisistaan.

Federointi ja kertakirjautuminen ovat toisiinsa liittyviä toiminnallisuuksia, jotka kuuluvat myös todentamisen ja valtuuttamisen alle, mutta ovat aihepiireinään niin merkittäviä, että ne käsitellään tässä erikseen. Federoinnissa keskeistä on eri organisaatioiden välinen luottamussuhde, joka mahdollistaa todentamis- ja identiteettitietojen luotettavan välittämisen näiden eri tahojen välillä. Näin kaikkien federoinnin piirissä olevien tahojen ei tarvitse pitää omaa käyttäjärekisteriä kaikkien muiden tahojen käyttäjistä, jotka mahdollisesti vierailevat heidän järjestelmissään. Lisäksi federointi mahdollistaa koko todentamisprosessin ulkoistamisen ulkopuoliselle taholle, mikä säästää todennusmekanismin suunnittelu- ja toteutuskustannuksissa. Federoinnissa käytetään laajalti SAML-protokollaa eri tahojen väliseen todennus- ja valtuutustiedon välitykseen, mutta federoinnissa voidaan käyttää myös esimerkiksi OpenID-standardia, joka mahdollistaa eri identiteetintarjoajan valitsemisen jokaiselle identiteettitransaktiolle.

Kertakirjautuminen tarkoittaa, että kohteet todentavat itsensä vain kerran kertakirjautumiskomponentille, joka sitten hoitaa kirjautumisen kaikkiin sen piirissä olevien kohdejärjestelmiin. Näin käyttäjien ei tarvitse muistaa tai kirjoittaa useita eri salasanoja useisiin eri järjestelmiin. Kertakirjautumistyypeistä yleisimpiä ovat verkko- ja yrityskertakirjautuminen. Ensimmäisellä tarkoitetaan selaimella tapahtuvaa kirjautumista verkkopalveluihin ja jälkimmäisellä taas yrityksen sisäisiin järjestelmiin kirjautumista. Yrityskertakirjautuminen toteutetaan usein joko käyttöjärjestelmäkertakirjautumisella tai sitten federoidulla kertakirjautumisella. Tämä jälkimmäinen yhdistää kertakirjautumisen federointiin. Käyttöjärjestelmäkertakirjautumiseen käytetään muun muassa SSPI-ohjelmointirajapintaa Windows-järjestelmissä ja GSSAPI-ohjelmointirajapintaa UNIX-pohjaisissa käyttöjärjestelmissä. Federoituun kertakirjautumiseen käytetään taas usein Kerberos-protokollaa tai Microsoft Active Directory Federation Service -palvelua.

Identiteetinhallinnan puolella tärkeimpiä toiminnallisuuksia ja osia ovat provisiointi, dentiteettien hallinnointi ja hakemistot. Provisiointi käsittää identiteettien luomisen, päivittämisen tai muokkaamisen ja poistamisen. Se voidaan toteuttaa muun muassa SPML- tai SCIM-protokollilla, joista molemmat kykenevät kaikkiin provisioinnissa tarvittaviin perustoimiin. SPML-protokolla ei kuitenkaan koskaan ole saavuttanut suurta suosiota ja nykyään etenkin pilvipalveluntarjoajat kritisoivat sitä XML-pohjaisuuden tuomasta monimutkaisuudesta ja raskaudesta. SCIM-protokollaa taas on kehitetty nimenomaan pilvipalvelujen vaatimukset mielessä ja se perustuu näin ollen alati yleistyvään REST-arkkitehtuuriin ja käyttää yksinkertaisia HTTP-protokollan metodeja toiminnassa. Identiteettien hallinnointi tarkoittaa identiteeteille suoritettavien toimien, kuten luomisen ja käyttöoikeuksien myöntämisen, valvomista erilaisilla politiikoilla. Siihen voidaan käyttää esimerkiksi XACML-standardia, jonka avulla voidaan

luoda yksityiskohtaisia pääsynhallintasääntöjä – esimerkiksi kuka tietoa saa käsitellä, miten ja mihin kellonaikaan.

Hakemistot, tai hakemistopalvelut, tarjoavat identiteetin- ja pääsynhallinnassa tarvittavat käyttäjätietokannat. Hakemistot ovat yleensä hierarkkisia ja puurakenteisia tietokantoja, jotka optimoidaan nopeisiin kyselyoperaatioihin. Koska etenkin isommilla organisaatioilla on tarve useille hakemistoille muodostuu näiden eri tietokantojen tietojen yhtenäisyyden ja ajantasaisuuden ylläpitäminen ongelmalliseksi. Helpotukseksi tähän voidaan käyttää metahakemistoja tai virtuaalihakemistoja, jotka molemmat luovat aggregoidun näkymän useista eri tietokannoista. Metahakemistot toteuttavat tämän fyysisesti ja virtuaalihakemistot loogisesti. Tämän vuoksi metahakemistot saattavat kärsiä useammista ongelmista kuin virtuaalihakemistot, jotka vain tekevät reaaliaikaisia hakuja ja muutoksia alkuperäisiin hakemistoihin säilyttämättä itse mitään varsinaista tietokantaa. Useat hakemistot perustuvat hierarkkiseen X.500-hakemistostandardiin, ja niitä yleensä käsitellään LDAP-hakemistonhallintaprotokollan avulla, joka tarjoaa rajalliset mutta kevyet ja tehokkaat kysely-, päivitys sekä todentamis- ja kontrollioperaatiot.

Yhdistelemällä tässä pääluvussa käsiteltyjä teknologioita, voidaan muodostaa kokonaisia identiteetin- ja pääsynhallintajärjestelmiä. Esimerkiksi yksinkertainen yrityksen tarpeisiin soveltuvan järjestelmän ytimessä voi olla LDAP-protokollalla hallinnoitava hakemistopalvelu, jonne kaikki käyttäjäidentiteetit ja näihin sidotut valtuustiedot on tallennettuina. Identiteetinhallintajärjestelmä voi luoda, muokata, hakea ja poistaa käyttäjätietoja sekä sisäisesti että kohdejärjestelmiin käyttäen SPML-protokollaa. Yrityksen työntekijät voivat kertakirjautua yrityksen järjestelmiin federoidusti pääsynhallintajärjestelmän kautta, joka puolestaan välittää todennus- ja valtuustiedot esimerkiksi SAML- tai Kerberos-protokollalla. Työntekijöiden suorittamaa identiteettien käyttöä voidaan valvoa ja rajoittaa XACML-standardilla luoduilla pääsynhallintapoliitikoilla. Yllä annettu esimerkki on yksinkertaistettu ja jättää huomioimatta muun muassa identiteetinhallintajärjestelmän sisäistä logiikkaa sekä eri palvelujen välissä mahdollisesti tarvittavat liittimet tai adapterit, mutta se sitoo yhtenäiseen ja todelliseen kontekstiin tässä luvussa esiteltyjä teknologioita.

4 Käyttäjä- ja pääsynhallintajärjestelmien esittelyä

Tässä luvussa esitellään identiteetinhallintajärjestelmän yleistettyä arkkitehtuuria ja sen osia. Arkkitehtuurin lisäksi esitellään myös markkinoilla olevia yleisimpiä käyttäjänhallintajärjestelmiä. Ensimmäisessä alaluvussa esitellään yleistä käyttäjänhallintajärjestelmän arkkitehtuuria ja toisessa vertaillaan eri valmistajien käyttäjä- ja pääsynhallintahallintasovelluksia.

4.1 Identiteetinhallintajärjestelmän yleistetty arkkitehtuurikuvaus

Tämä luku käsittelee identiteetinhallintajärjestelmän yleistä arkkitehtuuria kuvassa 12 esitetyn esimerkin kautta. Esimerkissä kuvattu järjestelmä esitellään seuraavaksi osa kerrallaan korkean tason näkökulmasta.

Lähdejärjestelmät

Tyypillisesti identiteetinhallintapalvelu liitetään yhteen tai useampaan autoritaariseen lähdejärjestelmään (engl. authoritative source), josta identiteettitiedot saadaan palveluun. Yksi yleisimmistä lähdejärjestelmistä on henkilöstöhallinnan tietojärjestelmä, josta saadaan perustiedot työntekijöistä ja heidän työsuhteistaan sekä yrityksen organisaatiorakenteesta. Lisäksi lähdejärjestelminä voidaan käyttää muun muassa asiakas-, kumppani-, alihankkija- ja sopimustietokantoja. [42, s. 6]

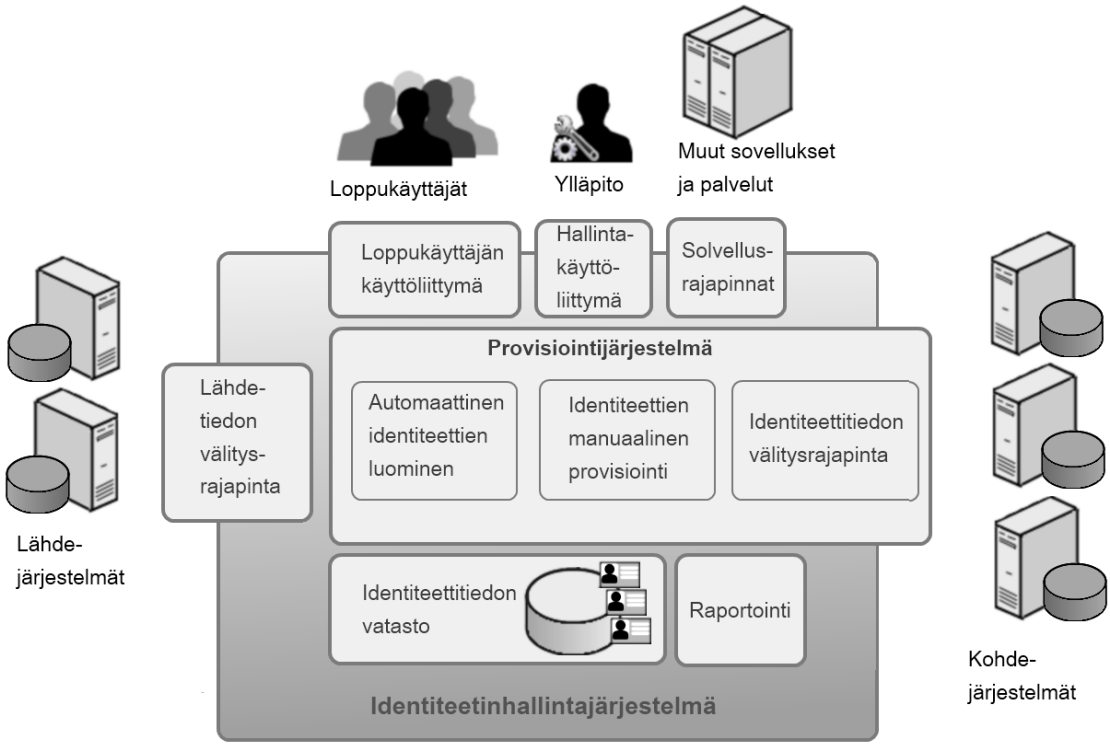
Lähdetiedon välitysrajapinta

Lähdetiedon välitysrajapinta vastaa lähdejärjestelmistä tuotavan lähdetiedon välittämisestä identiteetinhallintapalvelulle. Sen toteutuksessa voidaan käyttää tuote- tai teknologiakohtaisia liittimiä (engl. connectors) tai esimerkiksi yhteys- ja välitaulua lähdejärjestelmän tai identiteetinhallintapalvelun tietokannassa. Välityksessä voidaan käyttää myös esimerkiksi csv- tai xml-muotoisia tiedostoja. [42, s. 6] Lähdejärjestelmän autoritaarisuudella tarkoitetaan sitä, että mikäli identiteetinhallintajärjestelmän sisältämät identiteettitiedot eroavat tai ovat ristiriidassa lähdejärjestelmistä saatavan tiedon kanssa, lähdejärjestelmistä saatava tieto ratkaisee ja ristiriidassa olevat tiedot yleensä ylikirjoitetaan.

Provisiointijärjestelmä

Identiteetinhallintajärjestelmä luo lähdejärjestelmistä tulevan identiteettitiedon pohjalta omat identiteettinsä. Nämä identiteetit perustuvat lähdejärjestelmistä saatuun tietoon, mutta tämän lisäksi niille voidaan automaattisesti luoda identiteetinhallintajärjestelmän sisäiset identiteettitiedot, kuten loppukäyttäjän käyttäjätunnukset, sähköpostiosoitteet sekä pääsyoikeudet, joko yksittäisinä tai esimerkiksi rooli- tai ryhmäjäsenyyksinä. [43, s. 4][43, Liite]

Järjestelmän sisäisten tietojen lisäksi identiteeteille voidaan provisioida automaattisesti käyttäjätunnukset ja käyttövaltuudet kohdejärjestelmiin, kuten esimerkiksi sähköpostipalveluun ja sisäiseen verkkoportaaliin, identiteettitiedon välitysrajapinnan kautta. Välittäminen tapahtuu yleensä joko järjestelmäkohtaisten räätälöityjen liittimien kautta tai käyttämällä jotain yleiskäyttöistä provisiointimekanismia, kuten esimerkiksi keskitettyä käyttäjähakemistoa, johon kohdejärjestelmät voivat valtuutuspäätöksissään



Kuva 12. Esimerkki identiteetinhallinnan arkkitehtuurista [42, s. 9][44, s. 1]

tukeutua. Nämä keskitetyt käyttäjähakemistot voidaan toteuttaa käyttämällä esimerkiksi luvussa 3.5 mainittuja LDAP-hakemistoja. Järjestelmäkohtaiset liitokset voidaan taas toteuttaa esimerkiksi SPML-provisiointiprotokollalla. [43, s. 4]

Kaikkea provisiointia ei voida välttämättä toteuttaa automaattisesti kaikkiin kohdejärjestelmiin, joten provisiointijärjestelmä voi sisältää myös manuaalisen provisioinnin mahdollisuuden. Tällöin liittimien tai keskitettyjen hakemistojen sijasta provisiointiin käytetään muita työnohjauksen välineitä kuten sähköpostia. Tämä tarkoittaa, että provisioinnista vastaa joku henkilö, esimerkiksi kohdejärjestelmän ylläpitäjä, joka luo, päivittää ja poistaa identiteetit järjestelmään käsin. [43, s. 4]

Identiteettitiedon varasto

Identiteettitiedon varastot kuvaavat keskitettyjä tietovarastoja, joihin identiteetinhallintapalvelun tarvitsema identiteettitieto, kuten käyttäjäidentiteetit ja niille myönnetyt käyttövaltuudet, sekä muut resurssit, talletetaan. Tietovarastoina käytetään yleensä relaatiotietokantoja tai hakemistoja, usein LDAP-hakemistoa. Koska identiteettitiedon varastoissa oleva tieto on koko järjestelmän toimivuuden kannalta hyvin tärkeää, ulkopuoliset yhteydet näihin kantoihin ja hakemistoihin on useimmiten suljettu. Tällöin niiden tietoja käsitellään yksinomaan identiteetinhallintajärjestelmän sisäisten palveluiden välityksellä. [42, s. 5]

Loppukäyttäjän käyttöliittymä

Loppukäyttäjille tarjotaan käyttöliittymän välityksellä yleensä vähintään mahdollisuus nähdä ja hallita omia tietojaan. Lisäksi esimiesasemassa olevat henkilöt voivat tyypillisesti nähdä ja hallita alaistensa tietoja. Käytännössä omien tai alaisten tietojen katse-

lulla ja hallinnalla tarkoitetaan useimmiten henkilötietojen ja voimassaolevien käyttövaltuuksien katselua tai raportointia, uusien käyttövaltuuksien pyytämistä sekä käyttövaltuuspyyntöjen seurantaa ja hyväksymistä. [42, s. 6]

Yllä mainittujen peruskäyttöliittymätoimintojen lisäksi osa identiteetinhallintapalveluista tarjoaa loppukäyttäjille myös mahdollisuuden mallintaa ja hallita palvelun piirissä olevia käyttövaltuusrakenteita, sekä niihin liittyviä sääntöjä, rajoitteita ja työnkulkuja. Tämä mahdollistaa sen, että identiteetinhallinta voidaan delegoida käyttäjäorganisaatioon, eikä erillistä tahoa, joka myöntäisi käyttöoikeuksia, välttämättä tarvita. [42, s. 6]

Loppukäyttäjillä tarkoitetaan tässä yhteydessä pääasiassa organisaation omia työntekijöitä, mutta enenevässä määrin myös erilaisia organisaation ulkopuolisia käyttäjiä, kuten alihankkijoita, kumppaneita, asiakkaita tai ulkoisia auditoijia. Näille organisaation ulkopuolisille käyttäjille tarjotaan yleensä vain rajattu joukko käyttöliittymätoiminnallisuuksia. [42, s. 7]

Loppukäyttäjän käyttöliittymän käytettävyys (engl. usability) on koko identiteetinhallinnan käytännön toimivuuden kannalta hyvin tärkeää. Loppukäyttäjille tarjottavan näkymän on oltava riittävän selkeä ja helposti opittavissa, mikäli identiteetinhallinta delegoinnin halutaan onnistuvan. Loppukäyttäjän käyttöliittymä voidaan esimerkiksi integroida osaksi yritysportaalia tai sähköistä työpöytää, jotta käyttökokemus saataisiin mahdollisimman saumattomaksi. [42, s. 7]

Hallintakäyttöliittymä

Hallintakäyttöliittymällä tarkoitetaan yleensä erillistä käyttöliittymää identiteetinhallintapalvelun ylläpitohenkilöstölle. Sen tarkoitus on mahdollistaa palvelun konfiguraatioiden hallinta ja tästä syystä sen käyttö vaatiikin usein perehtyneisyyttä palvelun toteutuksessa käytettyihin tuotteisiin ja teknologioihin toisin kuin loppukäyttäjän käyttöliittymä. [42, s. 7]

Sovellusrajapinnat

Mikäli identiteetinhallintapalvelua halutaan käyttää myös muista sovelluksista tai palveluista käsin, tarvitaan erilaisia sovellusrajapintoja, jotka toimivat tulkkina sovelluksen ja identiteetinhallintapalvelun välillä. Sovellusrajapinta tarjoaa usein samoja toimintoja kuin loppukäyttäjän käyttöliittymäkin. [42, s. 7]

Raportointi

Raportointijärjestelmä mahdollistaa raporttien muodostamisen identiteetinhallintajärjestelmään kuuluvista identiteeteistä ja niiden tiedoista [44, s. 2]. Tällainen raportti voi sisältää esimerkiksi kaikkien identiteettitiedon varastoon tallennettujen käyttäjien kaikki eri tilit ja käyttövaltuudet tai vaihtoehtoisesti vain yksittäisen käyttäjän alaisten tiedot. Keskitetty raportointijärjestelmä voi kerätä ja yhdistellä tietoja eri osista identiteetin- tai pääsynhallintajärjestelmää ja antaa näin yhtenäisen näkymän muutoin hajanaisiin tietoihin, mistä on hyötyä mahdollisten ongelmien selvittämisessä ja auditoinnissa [44, s. 2].

Kohdejärjestelmät

Kohdejärjestelmät ovat mitä tahansa järjestelmiä, jotka käyttävät identiteetinhallintajärjestelmän tarjoamia identiteettitietoja [43, s. 4]. Esimerkiksi kulunvalvontajärjestelmät, sähköpostipalvelut, palkanlaskentajärjestelmät, käyttöjärjestelmät, keskitetyt käyttäjähakemistot sekä kaikki muut identiteettitietoja käyttävät järjestelmät voivat toimia kohdejärjestelminä, jos ne liitetään identiteetinhallintajärjestelmään [43, Liite]

4.2 Identiteetinhallintatuotteiden esittelyä ja vertailua

Tässä alaluvussa esitellään muutamien tunnetuimpien identiteetinhallintajärjestelmien valmistajien tuotteita ja vertaillaan niiden kyvykkyyksiä toisiinsa eri osa-alueilla. Vertailu perustuu Forrester Inc. -tutkimusyhtiön vuonna 2009 tekemään tutkimukseen identiteetinhallintajärjestelmistä [45].Vertailussa olivat mukana seuraavat yritykset: CA Technologies, Courion Corporation, Hitachi ID Systems, IBM, Microsoft, Novell, Oracle, SAP ja Sun Microsystems. Tutkimuksessa tuotteet pisteytettiin valmistajille esitettyjenä kyselyjen, tuotteiden demonstraatiotilaisuuksien sekä tuotteista asiakkailta saatujen arvioiden pohjalta. Tämä luku esittelee aluksi tutkimuksen tulokset tuotteiden tarjoamien toiminnallisuuksien ja ominaisuuksien suhteen ja siirtyy sitten niistä tehtäviin johtopäätöksiin.

Vertailun tulokset eri valmistajien identiteetinhallintatuotteiden tarjoamista ominaisuuksista arvioiduissa kategorioissa on esitetty kuvassa 13. Ylimmällä rivillä esitetään kunkin valmistajan tuotteiden ominaisuuksien saama painotettu keskiarvosana arvosanoista asteikolla 0 – 5, heikosta vahvaan, missä 0 tarkoittaa, ettei ominaisuutta ole lainkaan. Arvosteltavat ominaisuudet on esitetty kuvassa olevan taulun ensimmäisessä sarakkeessa ja niiden painoarvot toisessa.

	Painoarvo	CA	Courion	Hitachi ID Systems	IBM	Microsoft	Novell	Oracle	SAP	Sun Microsystems
TARJOTUT OMINAISUUDET		3.49	2.89	2.25	3.25	1.13	3.39	4.08	1.34	3.42
Käyttäjätilien provisiointi	25%	4.10	3.20	3.20	3.60	1.10	4.30	4.30	1.80	2.90
Roolienhallinta	10%	4.35	3.75	1.40	2.30	0.80	4.25	4.05	1.25	4.20
Verkkoyhteyksien hallinta (engl. WAM)	10%	5.00	2.30	2.30	3.80	3.00	3.05	4.10	0.00	4.30
Verkkopalvelujen turvallisuus	5%	4.30	2.00	2.00	5.00	2.80	4.10	3.40	0.00	3.40
Federointi	5%	2.35	1.40	1.40	4.25	1.40	2.80	3.25	0.00	3.85
Käyttövaltuuksien valvonta	10%	2.15	2.40	2.40	3.30	0.00	0.60	4.40	0.00	3.85
Yrityskertakirjautuminen (E-SSO)	5%	3.10	1.50	4.60	5.00	0.00	3.10	3.60	0.00	0.90
Hakemisto/Virtuaalihakemisto	10%	2.00	4.30	0.00	0.60	1.00	3.70	4.10	4.40	4.40
Raportointi	5%	3.80	2.60	1.80	5.00	0.00	3.40	4.60	0.80	2.20
Muut ominaisuudet	5%	3.10	1.50	0.70	4.10	0.50	3.10	4.10	1.70	2.10
Asiakkaiden suosittelut	10%	2.80	3.60	3.10	1.85	1.40	3.30	3.90	2.00	4.00

Pisteytykset perustuvat asteikolle 0 – 5 (heikko – vahva)

Kuva 13 Eri valmistajien identiteetinhallintatuotteiden vertailun tulokset [45, kuva 3]

Tutkimuksessa saatujen tulosten keskiarvosanojen perusteella voidaan tehdä suurpiirteistä jakoa valmistajien tuotteiden keskinäisestä paremmuudesta kokonaiskyvykkyyden suhteen. Jos valmistajien tuotteet jaetaan arvosanavälikategorioihin, parhaaseen

4–5 -kategoriaan sijoittuu vain yhden valmistajan, Oraclen, tuotteet. Toiseen 3–4 -kategoriaan sijoittuu kuitenkin jo neljän valmistajan, CA:n, Sun Microsystemsin, Novellin ja IBM:n, tuotteet arvosanan suuruusjärjestyksessä mainittuina. Kolmanteen kategoriaan, 2–3, sijoittuvat Courionin ja Hitachi ID Systemsin tuotteet. Tulosten viimeiseen kategoriaan, 1–2, sijoittuvat kahden valmistajan, SAP:n ja Microsoftin, tuotteet. Yhteenvetona hieman yli puolet valmistajista (~56%) saa tuotteilleen paremman arvosanan kuin 3, jolloin näiden tuotteiden kokonaiskyvykkyyksiä voidaan pitää vähintään tyydyttävinä tai sitä parempina. Loppujen neljän valmistajan tuotteet (~44%) voidaan vastaavasti kategorisoida kokonaiskyvykkyydeltään välttäviksi tai sitä heikommiksi.

Tuloksia tarkemmin tarkastellessa voidaan kuitenkin havaita muita mielenkiintoisia piirteitä arvostelluista tuotteista. Esimerkiksi yksittäisten valmistajien sarakkeita tarkastellessa voidaan huomata, että hyvästä tai heikosta keskiarvosanasta huolimatta useimmilla valmistajilla on selkeitä yksilöllisiä vahvuuksia ja heikkouksia tuotteissaan, eikä osa valmistajista myöskään tarjoa kaikkia arvosteltavista ominaisuuksista, mikä laskee niiden keskiarvosanaa. SAP:n identiteetinhallintatuotteet ovat hyvä esimerkkitapaus tästä, sillä niiden saama pistemäärä hakemiston tai virtuaalihakemiston toteuttamisesta on tulosten korkein, mutta kokonaisarvosana jää taas arvostelun toiseksi heikoimmaksi. Näiden vääristymien vuoksi jokaisen valmistajan tuotteiden pistemääräjakaumille piirrettiin yksilökohtaiset kuvaajat, jotta niiden vahvuudet ja heikkoudet tulisivat paremmin esiin. Kuvaajatyypiksi valittiin viivakuvaaja, koska se helpottaa visuaalista vertailua kuvaajien kesken. Kuvaajat on esitetty kuvassa 14.

Seuraavaksi käydään läpi jokaisen valmistajan tuotteet lyhyesti kuvaan 14 piirrettyjen kuvaajien valossa. Yksinkertaisuuden vuoksi tässä läpikäynnissä kyvykkyydet jaetaan seuraaviin luokkiin: vahvaan (arvosana ≥ 4), tyydyttävään ($3 \leq$ arvosana < 4) ja heikkoon (arvosana < 3).

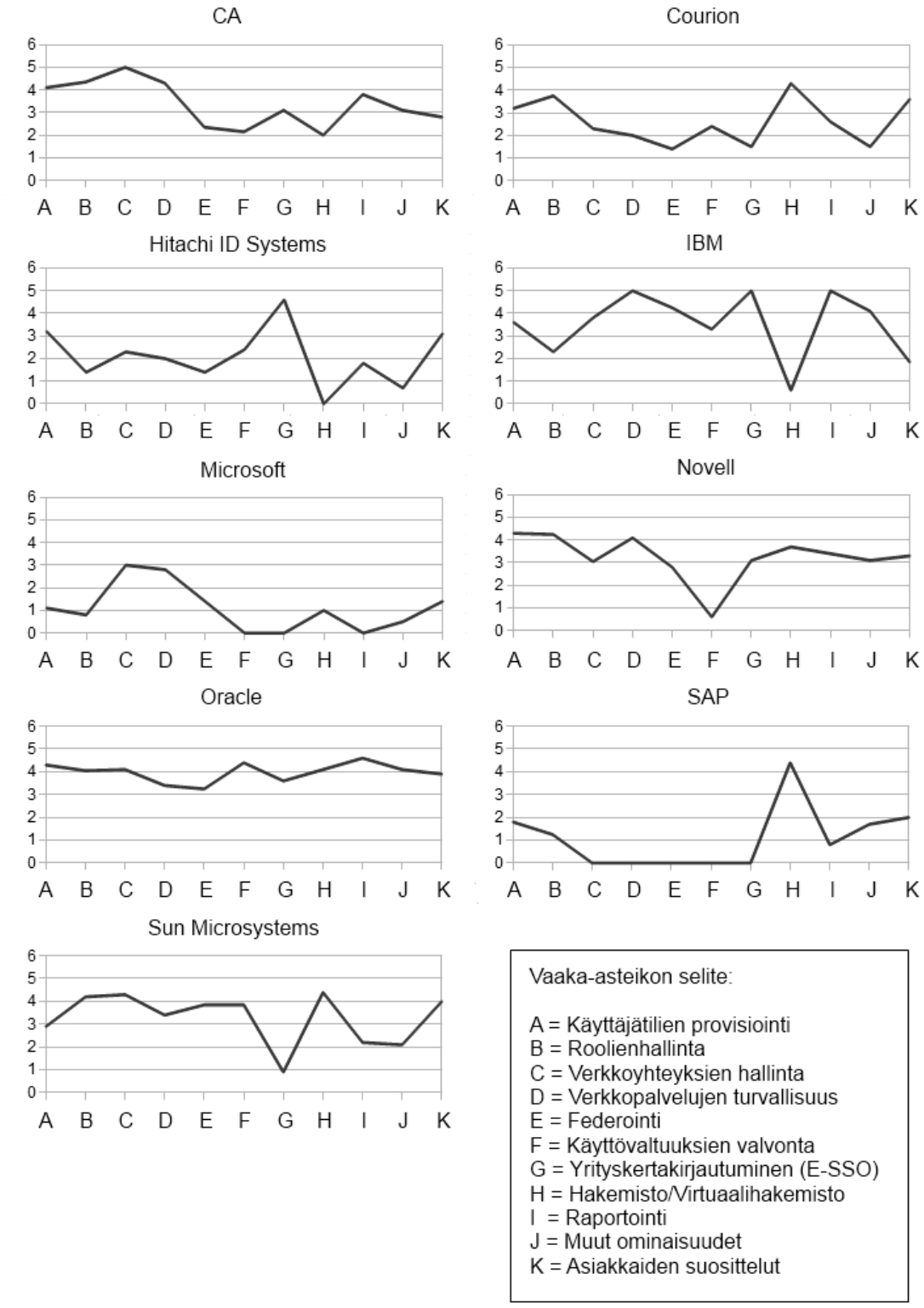
CA:n tuotteiden vahvuudet ovat neljässä ensimmäisessä ominaisuudessa: käyttäjätilien provisioinnissa, roolienhallinnassa, verkkoyhteyksien hallinnassa ja verkkopalvelujen turvallisuudessa. Verkkoyhteyksien hallinnan kyvykkyys on erityismaininnan arvoinen, koska se sai täyden 5:n arvosanan ainoana arvostelluista tuotteista. CA:n tuotteet saavat tyydyttävän kyvykkyyden raportoinnin, yrityskertakirjautumisen ja muiden ominaisuuksien osalta, mutta hakemistojen, federoinnin ja käyttövaltuuksien valvonta jäävät puolestaan heikoiksi. Yhteenvetona CA:lla on vahva pohja provisiontipuolella ja verkkopalvelujen sekä -yhteyksien turvallisuudessa, mutta etenkin käyttövaltuuksien valvonnassa ja hakemistopalveluissa olisi parantamisen varaa.

Courionin tuotteilla ei näy olevan muita vahvoja kyvykkyyksiä kuin hakemistojen toteutus. Käyttäjien provisiointi ja roolienhallinta ovat tyydyttävällä tasolla ja asiakkaiden suosittelut ovat tutkimuksen kolmanneksi korkeimmat. Muut ominaisuudet jäävät kyvykkyydeltään heikoiksi. Yhteenvetona Courionin tuotteet voivat tarjota kyvykkään hakemistopalvelun ja kohtuullisen provisiointipohjan, mutta esimerkiksi pääsynhallintapuoli kaipaisi vahvistusta.

Hitachi ID Systemsin tuotteilla ei myöskään vaikuta olevan kuin yksi vahva ominaisuus: yrityskertakirjautuminen. Käyttäjätilien provisiointi ja asiakkaiden suosittelu ovat tyydyttävällä tasolla, mutta kaikki muut omaisuudet jäävät heikoiksi. Erikoista on, että Hitachi ID Systems ei tarjoa lainkaan hakemistopalvelua, joka toimii yhtenä identiteetinhallinnan arkkitehtuurillisista peruspilareista. Yhteenvetona Hitachi ID

Systems tarjoaa hyvän yrityskertakirjautumisen, mutta koska sen muu tarjonta on heikkoa, vaikuttaa se soveltuvan hyvin vain tähän yhteen käyttötarkoitukseen.

Kuva 14 Eri valmistajien identiteetinhallintatuotteiden yksilökohtaiset pistemääräja-



kaumat.

IBM:n tuotteet saavat tutkimuksen parhaat arvostelut täydellä 5:n arvosanalla peräti kolmesta eri kategoriasta: verkkopalvelujen turvallisuudesta, yrityskertakirjautumisesta ja raportoinnista. Näiden lisäksi federointi ja muut ominaisuudet arvostellaan vahvoiksi. Provisiointi, verkkoyhteyksien hallinta ja käyttövaltuuksien hallinta ovat tyydyttävällä tasolla. Roolienhallinta jää heikoksi ja hakemistopalvelut saavat tutkimuksen huonoimmat, hyvin heikot, arvostelut. Lisäksi IBM:n tuotteet saavat varsin heikot pisteet asiakkailta tutkimuksen toiseksi huonoimmilla arvosteluilla, mikä voi viitata esimerkiksi heikkoon käytettävyyteen, jota ei erikseen tutkimuksessa arvioitu. Yhteenvetona IBM:n tuotteet tarjoavat siis monipuolisia ja kyvykkyydeltään hyviä ominaisuuksia, etenkin pääsynhallinnan puolella, mutta sen hakemistopalvelut ovat poikkeuksellisen huonot, ja tuotteet saavat asiakkailta melko huonoa palautetta suosittelujen muodossa.

Microsoftin tuotteet ovat poikkeuksellisia siinä, että niillä ei ole yhtään vahvaa ominaisuutta ja tyydyttäviäkin ominaisuuksia on vain yksi: verkkoyhteyksien hallinta. Roolienhallintaa, käyttövaltuuksien valvontaa, yrityskertakirjautumista, raportointia tai muita ominaisuuksia ei tarjota lainkaan. Lopuissakin ominaisuuksissa on muihin tuotteisiin vertailtuna varsin huonot arvosanat. Asiakkaiden palaute tuotteista on lisäksi tutkimuksen heikoin. Yhteenvetona Microsoftin tuotteet vaikuttavat soveltuvan hyvin heikosti identiteetinhallintaan ja asiakkaiden suosituksien alhainen arvosana on sen mukainen.

Novellin tuotteiden vahvuudet ovat käyttäjien provisioinnissa, roolienhallinnassa ja verkkoyhteyksien turvallisuudessa. Ainoastaan federointi ja käyttövaltuuksien hallinta saavat heikot arvostelut ja kaikki loput ovat tyydyttäviä. Yhteenvetona Novell ei loista yksittäisillä osa-alueilla muihin valmistajiin verrattuna, mutta onnistuu tarjoamaan varsin tasapainoisen tuotteen, jolla on vähintään tyydyttävä kyvykkyys lähes joka osa-alueella. Käyttövaltuuksien hallinta on kuitenkin syytä nostaa esiin merkittävänä heikkoutena, koska se sai tutkimuksen huonoimman arvion kaikista niistä tuotteista, jotka sitä tarjosivat.

Oraclen tuotteiden kuvaajasta voidaan nopeasti nähdä, että se tarjoaa kaikkein tasapainoisimman ja vieläpä poikkeuksellisen kyvykkään kokonaisuuden. Sillä on kaikista valmistajista eniten vahvoiksi luokiteltuja ominaisuuksia: provisiointi, roolienhallinta, verkkoyhteyksien hallinta, käyttövaltuuksien hallinta, hakemistot, raportointi sekä muut ominaisuudet. Kaikki loput ominaisuudet ovat tyydyttäviä, eikä heikkoja tai puuttuvia ominaisuuksia ole lainkaan. Asiakkaiden antamat suosittelutkin ovat tutkimuksen toiseksi parhaat, joten Oraclen tuotteiden voidaan näiden tietojen pohjalta todeta ansainneen keskiarvosanansa suoman ensimmäisen sijan vertailussa.

SAP:n tuotteilla on, kuten aiemmin luvussa mainittiin, vain yksi vahvuus eli hakemistopalvelu. Tästä yksittäisestä vahvuudesta SAP kuitenkin saa tutkimuksen parhaan arvosanan. Tyydyttäviä ominaisuuksia ei ole lainkaan ja suurinta osaa arvostelluista ominaisuuksista ei edes tarjota. Ainoastaan käyttäjien provisiointi, roolienhallinta sekä muut ominaisuudet saavat hakemistojen lisäksi arvosanan, ja nämäkin kaikki ominaisuudet ovat heikkoja. Asiakkaiden suositukset ovat keskivertoa alemmat. Yhteenvetona SAP:n identiteetinhallintatuotteet eivät tarjoa moniakaan identiteetinhallinnan kannalta keskeisiä ominaisuuksia, mutta ne tarjoavat todella hyvän hakemistopalvelun.

Sun Microsystemsin tuotteiden vahvuudet ovat roolienhallinnan, verkkoyhteyksien hallinnan ja hakemistojen saralla. Lisäksi se saa tutkimuksen parhaat suositukset asiakkailtaan. Tyydyttävällä tasolla olevia ominaisuuksia ovat verkkopalvelujen turvallisuus, federointi ja käyttövaltuuksien valvonta. Yrityskertakirjautumista ei tarjota lainkaan ja loput ominaisuudet jäävät heikoiksi. Sun Microsystemsin tuotteet ovat erikoisia siinä, että kaikissa muissa tuotteissa provisiointi on toteutettu paremmin tai vähintään yhtä hyvin kuin roolienhallinta, mutta Sun Microsystemsin tuotteissa provisiointi jää heikoksi vaikka roolienhallinta on tutkimuksen vahvimmasta päästä.

Tutkimuksessa arvostelluista tuotteista lähes kaikilla on vahvuutensa ja heikkoutensa paitsi Oraclella, joka tarjoaa tasapainoisimman ja keskimäärin kyvykkäimmän kokonaisuuden, joka ylittää muut tuotekokonaisuudet selkeästi. Tämän pohjalta Oracle olisi paras valinta kokonaisvaltaiseksi identiteetinhallintatuotteiden tarjoajaksi. Kuitenkin identiteetinhallinnan tarpeet voivat olla monimuotoisia ja tuotteiden joukosta erottuu myös tuotteita, joiden vahvuudet soveltuvat erittäin hyvin johonkin tiettyyn tarkoitukseen. SAP:n tuotteet soveltuvat parhaiten käyttäjähakemistopalvelun toteuttamiseen, IBM tarjoaa parhaan verkkopalvelujen turvallisuuden ja yrityskertakirjautumisen sekä raportointitoiminnallisuuden, CA:n tuotteilla saavutetaan paras verkkoyhteyksien hallinta, Novell jakaa parhaan sijan provisioinnista Oraclen kanssa jne. Tutkimus ei ota kantaa tuotteiden lisenssimaksuihin, mutta lienee kohtuullista olettaa, että yleisesti tuotteet, jotka tarjoavat monipuolisempia ominaisuuksia ovat lisenssimaksuiltaan kalliimpia kuin yksinkertaisemmat tuotteet. Yhdessä kaikki arvostellut tuotteet tarjoavat kyvykkyyksiltään kirjavan tarjonnan ominaisuuksia, josta organisaatiot voivat valita omiin tarpeisiinsa kustannuksiltaan sopivimman kokonaisuuden.

4.3 Yhteenveto

Identiteetinhallintajärjestelmien arkkitehtuuri koostuu yleisesti lähdejärjestelmistä, provisiointijärjestelmästä, identiteettitiedon varastosta, hallinta- sekä loppukäyttäjän käyttöliittymästä ja kohdejärjestelmistä. Lähdejärjestelmät ovat ne lähteet, joista identiteettitiedot alun perin saadaan järjestelmään. Lähdejärjestelmät liitetään identiteetinhallintajärjestelmään lähdetiedon välitysrajapinnan kautta erilaisilla liittimillä tai adaptereilla. Provisiointijärjestelmä luo lähdejärjestelmistä saadun tiedon pohjalta identiteetit identiteetinhallintajärjestelmään ja tallettaa ne identiteettitiedon varastoon eli yleensä johonkin hakemistoon. Identiteettitietojen hallinta järjestelmässä tapahtuu hallinta- ja loppukäyttäjän käyttöliittymien välityksellä. Kohdejärjestelmät ovat niitä järjestelmiä, jotka lopulta käyttävät identiteetinhallintajärjestelmän tarjoamia identiteettitietoja.

Nykyisten identiteetinhallintatuotekokonaisuuksien arvioiden perusteella tuotteiden kyvykkyydet eri osa-alueilla eroavat selkeästi eri valmistajien välillä. Arviossa arvosteltiin muun muassa käyttäjien provisiointia, roolienhallintaa, verkkoyhteyksien hallintaa, verkkoyhteyksien turvallisuutta, federointia, käyttövaltuuksien valvontaa, yrityskertakirjautumista, hakemistopalvelua, raportointia sekä asiakkaiden suositteluja asteikolla 1 – 5.

Sekä vahvin että kokonaisvaltaisesti tasalaatuisin arvostelluista tuotekokonaisuuksista oli Oracle keskiarvolla 4,08. Muita melko hyvin menestyneitä valmistajia olivat CA, Sun Microsystems, Novell ja IBM. CA erottui edukseen vertailun parhaalla verkkoyhteyksien hallinnalla (arvosana 5); IBM verkkopalvelujen turvallisuudella, yrityskertakirjautumisella sekä raportoinnilla (arvosana 5 kaikista); ja Sun Microsystems parhail-

la asiakasarvioillaan (arvosana 4). SAP:in tuotekokonaisuus oli kaikista rajoittunein ja sai pitkälti huonoimmat arvosanat kaikista muista osa-alueista paitsi hakemistopalvelusta, josta se sai taas arvostelun parhaan arvosanan, 4,4. SAP vaikuttaa siis äärimmäisen kapeasti mutta hyvin erikoistuneelta tuotekokonaisuudelta

Loppujen lopuksi ominaisuuksien ja niiden kyvykkyyksien valikoima tuotteiden kesken oli hyvin kirjava, mikä heijastaa ehkä myös yritysten tarpeiden monimuotoisuutta. Tämän vuoksi useimmista tuotteista ei suoraan voida sanoa, että ne olisivat huonompia kuin jokin toinen, koska juuri tietynlaisiin tarpeisiin ne voivat olla kaikista sopivin valinta. Lisäksi täytyy ottaa huomioon, ettei tutkimuksessa käsitelty tuotteiden hintaa, mikä voi nostaa hieman heikommin keskiarvosanaltaan menestyneiden tuotteiden houkuttelevuutta. Kukin organisaatio voi verrata omia tarpeitaan tässä luvussa esiteltyihin arvioihin tuotteiden kyvykkyyksistä osa-alueittain ja käyttää näitä tietoja hyväkseen tuotekokonaisuutensa valinnassa ottaen huomioon myös kustannukset ja muut tässä esittelemättömät asiat, jotka voivat vaikuttaa valintoihin.

5 Asiantuntijakysely identiteetin- ja pääsynhallinnan teknologioista

Tässä luvussa esitellään osana diplomityötä suoritettua asiantuntijakyselyä ja sen tuloksia. Luvussa selostaan aluksi kyselyn tarkoitus sekä kuvataan kyselyn metodologia ja sen toteutukseen liittyneet järjestelyt. Tämän jälkeen käsitellään itse kyselyn tuloksia ja analysoidaan niiden ohella myös kyselyn toimivuutta. Lopussa tehdään yhteenveto tuloksista ja niiden merkityksestä.

Kyselyn tarkoituksena oli kartoittaa asiantuntijoiden näkemyksiä identiteetin- ja pääsynhallinnasta sekä sen teknologisista toteutuksista. Kartoituksen pääpaino oli identiteetin- ja pääsynhallinnan vahvuuksien, heikkouksien ja uhkien selvittämisessä sekä nykyisten trendien merkityksen arvioimisessa teknologian tulevaisuuden kannalta. Kyselyn taustana toimi se, että näin laajan tieteenalan teknisestä kirjallisuudesta ja artikkeleista saadaan niin laaja ja hajautunut kuva teknologian tilasta, ettei siitä voida helposti muodostaa todellisuutta vastaavaa ja ajantasaista kuvaa käytännössä sovellettavasta teknologiasta ja sen tilasta. Näin ollen tämän asiantuntijakyselyn tulosten olisi tarkoitus täydentää kirjallista lähdemateriaalia ja auttaa kohdentamaan huomiota käytännön käyttötarkoitusten ja -tarpeiden kannalta tärkeisiin osa-alueisiin sekä vahvistamaan tai vastavuoroisesti heikentämään lähdemateriaalin pohjalta muodostuneita mielikuvia ja olettamuksia.

Kyselytutkimus toteutettiin Internetin välityksellä täytettävällä lomakkeella, jonka tarjosi palveluna Freeonlinesurveys.com [46]. Varsinainen kyselylomake (ks. Liite I) laadittiin sisältämään sekä suljettuja monivalintakysymyksiä että avoimia kysymyksiä. Monivalintakysymysten tarkoitus oli saada vastaajien kesken vertailukelpoisia vastauksia koskien muun muassa tiettyjen identiteetin- ja pääsynhallinnan teknologioiden kypsyyttä ja nykyisten trendien merkitystä teknologian kehityksessä. Avoimien kysymysten tarkoitus oli puolestaan luoda mahdollisuus saada uutta tietoa sekä poimia vastaajien kesken spontaanisti esiintyviä yhtenevyyksiä vastauksissa. Näiden lisäksi avoimien kysymysten yksi keskeinen tarkoitus oli antaa kvalitatiivista sisältöä kyselylle siltä varalta, ettei kvantitatiivisesta analyysistä saataisikaan käyttökelpoisia tuloksia vastausten vähyyden vuoksi.

Kyselyn kohderyhmänä olivat identiteetin- ja pääsynhallinnan asiantuntijat. Koska maantieteellistä rajausta ei haluttu tehdä vaan maksimoida potentiaalisten vastaajien määrä, toteutettiin kysely englanniksi. Tämä kielivalinta oli luonteva paitsi maailmanlaajuisen levikin vuoksi myös siksi, että aihepiirin vakiintunut termistö ja kirjallisuus ovat hyvin pitkälti englanninkielisiä, mikä pienentää entisestään todennäköisyyttä sille, että alan asiantuntijat eivät osaisi tarpeeksi kieltä kyselyyn vastatakseen.

Kyselyä lähetettiin suoraan useille yrityksille, jotka joko tarjoavat konsultointia identiteetin- ja pääsynhallinnan toteutukseen tai valmistavat tuotteita siihen. Koska tämä lähestymistapa ei tuottanut montaa vastausta lukuisista pyynnöistä ja muistutuksista huolimatta, välitettiin kyselyä myös henkilökohtaisissa kontaktiverkoissa sekä useissa LinkedIn-verkostoitumissivuston [47] identiteetin- ja pääsynhallinnan ryhmissä.

Kyselyyn osallistuneet henkilöt on nimetty aakkosjärjestyksessä alla olevassa listassa kiitoksena ja tunnustuksena heidän panoksestaan tälle tutkimukselle.

Clemmer, Lee

Davis, Jeff

Greb, Markus

Hegde, Nithin

Hurdalek, Milos

Koutaniemi, Hannu

Krishnan, Muthu

Kähkipuro, Pekka

Le, Sammy

Liebeck, Thomas

Lindqvist, Pekka

Nordvaller, Peder

Parry, Cameron

Pinkney, Simon

Reddy, Sudhakar

Riggins, Robert

Schwartz, Mike

Semenova, Natalia

St-Pierre, Nicolas

Tanskanen, Tapani

Vestergaard, Dahl, Peter

White, Jeremy

5.1 Kyselyn vastaajien demografiset tiedot

Vastaajilta kerättiin kyselyssä seuraavat demografiset tiedot: nimi, alan kokemus, yritys sekä maa. Tässä luvussa kuvataan esitellään näistä tiedoista saatuja tuloksia, joiden pohjalta varsinaisia vastauksia voidaan arvioida. Ensin esitellään vastaajien ja vastausten maantieteellistä jakaumaa ja sen jälkeen heidän työkokemustaan identiteetin- ja pääsynhallinnan parissa. Yksittäisiä vastauksia ei liitetty yksityisyydensuojasyistä keneenkään tiettyyn henkilöön, jotta vastaajat voisivat vastata vapaasti työn julkisesta luonteesta huolimatta. Kaiken kaikkiaan vastaajia oli 22, mikä vähäisyydes-

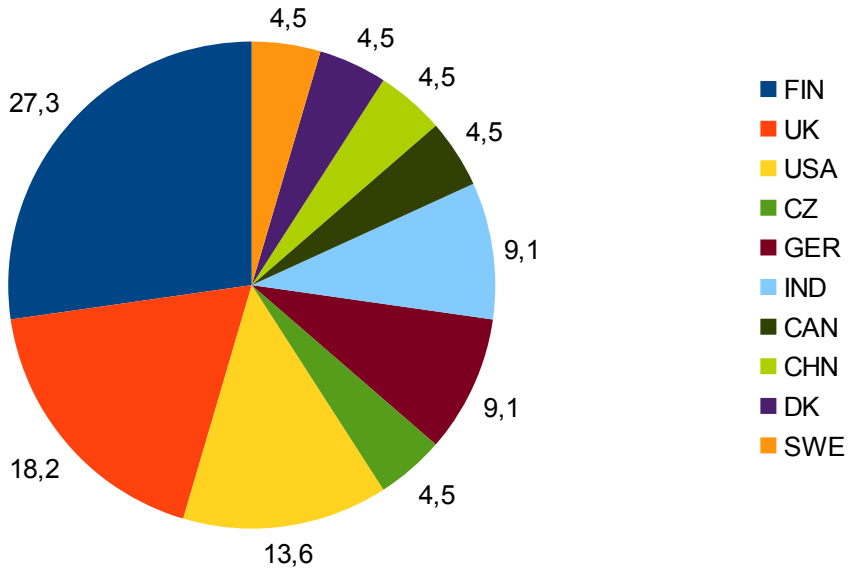
sään heikensi tulosten edustavuutta. Tätä vastaajamärän vähäisyyttä ja muita kyselyyn liittyneitä haasteita käsitellään lisää luvussa 5.4.

Kyselyn vastausten maantieteellistä jakaumaa voidaan tarkastella taulukosta 5.1 ja graafisesti havainnollistettuna kuvasta 15. Vaikka kyselyn tarkoitus olikin saada maantieteellisesti mahdollisimman laajasti jakautunut vastaajakunta, yllätti lopullinen jakauman monipuolisuus positiivisesti. Etenkin Aasian ja Pohjois-Amerikan manterei-den osallistumisen aste koettiin positiivisena, sillä vastausten arveltiin jäävän hyvin Eurooppa-keskeisiksi. Ilmeisesti LinkedIn-sivuston maailmanlaajuinen suosio auttoi tavoittamaan identiteetin- ja pääsynhallinnan asiantuntijoita joka puolelta maapalloa. Suomi jäi kuitenkin odotetusti eniten vastauksia tuottaneeksi maaksi johtuen henkilö-kohtaisen kontaktiverkoston keskittymisestä kotimaan alueelle, vaikka Yhdistynyt kuningaskunta ja Yhdysvallat seurasivatkin kohtuullisen hyvin perässä.

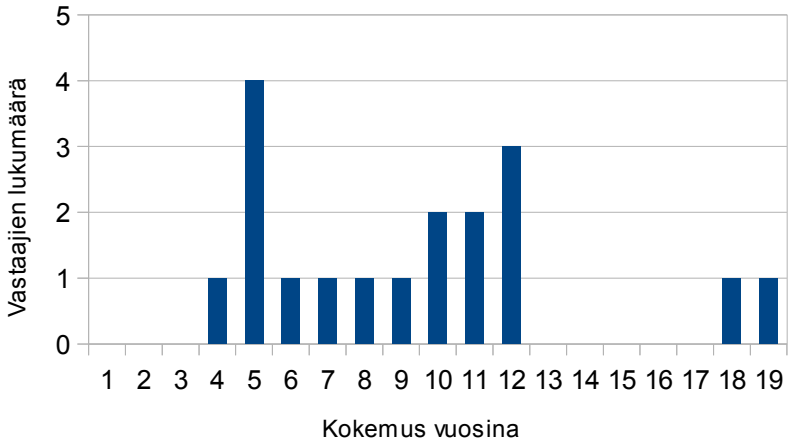
Vastanneista 17 (n. 77%) ilmoitti kokemuksensa vuosina ja nämä vastaukset on havainnollistettu kuvassa 16. Jakauman tunnusluvut on listattu taulukkoon 5.2. Kuten kuvan frekvenssijakaumasta voidaan nähdä, vastaajien työkokemus alalta painottui pääasiassa 4–12 vuoden välille, mutta näiden lisäksi mukana oli myös kaksi huomat-tavan pitkän uran ammattilaista 18 ja 19 vuoden työkokemuksilla. Vastaajien keski-määräinen työkokemus oli vastausten perusteella noin 9,4 vuotta, mikä tuki oletusta vastaajien asiantuntijuudesta.

Taulukko 5.1. Vastaajien maantieteellinen jakauma

Maat	Lukumää	%-osuus vastauksista
FIN	6	27,3
UK	4	18,2
USA	3	13,6
GER	2	9,1
IND	2	9,1
CZ	1	4,5
CAN	1	4,5
CHN	1	4,5
DK	1	4,5
SWE	1	4,5



Kuva 15. Vastausten maantieteellinen prosenttijakauma ympyrädiagrammina



Kuva 16. Vastaajien kokemuksen frekvenssijakauma (vuosia)

Taulukko 5.2. Vastaajien kokemuksen tunnusluvut

Keskiarvo	Mediaani	Standardipoikkeama
9,39	9,5	4,33

Kysymys kokemuksesta oli avoin, joten vuosina ilmoitettujen kokemuksien lisäksi vastauksista saatiin kerättyä hieman muutakin mielenkiintoista taustatietoa vastaajista. Useimpien vastaajien taustat keskittyivät odotetusti tekniseen toteutukseen ja suunnitteluun, mutta osalla oli myös sovelluskehityskokemusta sekä muutamalla kaupallistakin kokemusta alalta. Taustakertomuksista voitiin myös huomata, että kokemukset erosivat myös erikoistumisissa. Osa oli selvästi keskittynyt työssään pääsynhallintaan,

osa taas pääasiassa identiteetinhallintaan ja loput tasaisemmin molempiin osa-alueisiin. Kokemuskuvauksien pohjalta vastaajajoukossa vaikutti olevan monimuotoisuutta niin kokemuksen pituuden kuin myös erikoistumisen osalta, mitä voidaan ajatella edustavuuden kannalta hyvältä asiana, vaikka toisaalta erilaisuus voi helposti myös hajauttaa vastauksia ja tehdä johtopäätöksien tekemisestä haastavampaa.

5.2 Monivalintavastausten tulokset

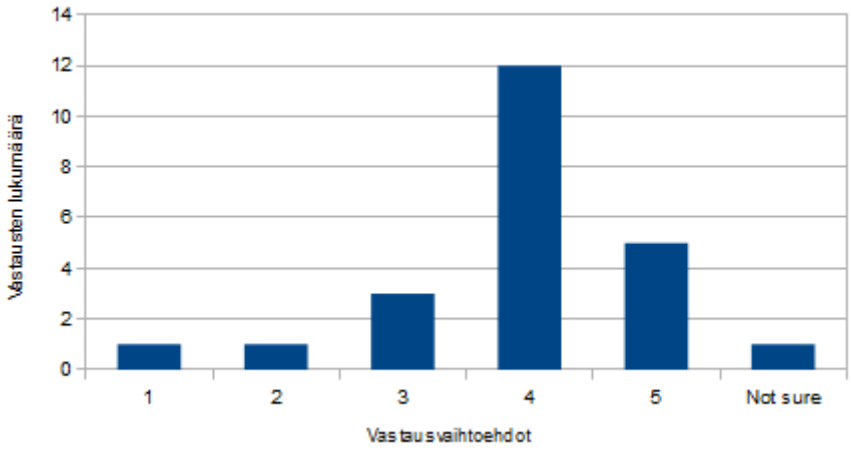
Tässä luvussa käsitellään kyselyssä olleiden monivalintakysymysten tuloksia. Monivalintakysymysten tarkoituksena oli mitata kvantitatiivisesti identiteetin- ja pääsynhallinnan eri osa-alueiden tai toiminnallisuuksien kypsyyttä ja pyrkiä selvittämään, mitkä niistä tarvitsisivat merkittävää parannusta ja mitkä eivät. Tällaista tietoa voitaisiin hyödyntää tuotekehittäjien kehityspäätösten tekemisessä ja auttaa näin kehittämään teknologiaa käytännön kannalta parempaan suuntaan.

Jokaisesta kysymyksestä on laskettu keskiarvo ja keskipoikkeama sekä luottamusväli, jotka ovat esillä taulukossa 5.3. 95%:n luottamusväli keskiarvoille on laskettu kaavalla 1 [48, luku 6], missä $\overline{x}$ tarkoittaa kysymyksen vastausten keskiarvoa, z taulukkolukua, s keskipoikkeamaa ja n otoskokoa. Koska vastausten otoskoko oli alle 30, käytettiin taulukkolukuna normaalijakauman sijasta t-jakaumaa n-1:n vapausasteella. Tällöin vapausasteita oli 21 ja z:n arvoksi saatiin 2,08. Taulukon keskiarvot ja keskipoikkeamat on laskettu suoraan OpenOffice Calc -taulukkolaskentaohjelmalla.”Not sure” -vastauksia ei ole laskettu mukaan, mikä on huomioitu laskemalla n kysymyskohtaisesti käyttökelpoisista vastauksista.

$$\overline{x} \pm z \frac{s}{\sqrt{(n)}} \tag{1}$$

Taulukon tuloksista voidaan nähdä, että vastausten vähäisen määrän vuoksi leveiksi jääneet luottamusvälit vaikeuttavat johtopäätöksien vetoa tuloksista. Muutamassa tapauksessa selkeitä linjanvetoja voidaan kuitenkin vetää. Ensimmäisen kysymyksen keskimääräinen vastauksen luottamusväli identiteetin- ja pääsynhallintajärjestelmien käyttöönoton ja konfiguroinnin vaikeudesta jää vähimmilläänkin 3,59:än, jota voidaan pitää jo merkittävästi keskimääräistä (3) vaikeampana. Kuvassa 17 jakaumaa on havainnollistettu pylväsdiagrammilla, jossa painottuneisuus 3:n suuremmalle puolelle on hyvin nähtävissä. Tulos tuskin on kovin yllättävä alan ammattilaisille, mutta se voi toimia hyvänä herätteenä tuotteiden valmistajille siitä, että nykyiset ratkaisut ovat tosiasiassa vaikeita ottaa käyttöön. Toiminnallisuuksien ja osien osalta hakemistopalvelut vaikuttavat olevan hyvällä mallilla, koska korkeimmillaankin vastauksen luottamusväli jää alle 2,5:n eli merkittäviä parannuksia ei tälle osa-alueelle vaikuta kaivattavan. Päinvastainen kuva saadaan puolestaan raportoinnista, jossa luottamusväli jää alimmillaankin yli 3,6:n, mikä kielii varsin merkittävien parannusten tarpeesta. Raportoinnin ohella muita parannusta kaipaavia ominaisuuksia ovat monitorointi, käytettävyys loppukäyttäjille, delegoitu hallinta sekä roolienhallinta, joiden kaikkien vastauksen luottamusväli jää alimmillaankin yli 3:n. Loppujen osien ja toiminnallisuuksien osalta näin selviä linjauksia ei voida vetää, koska niiden luottamusvälit sisältävät arvoja molemmin puolin 3:a.

Trendien suhteen saaduista tuloksista ei paljastu mitään mullistavaa. Kaikkien trendien luottamusvälit jäävät yli 3:n eli niitä voidaan pitää merkittävinä nykyisinä ja tulevina vaikuttajina identiteetin- ja pääsynhallinnan kehitykseen, mutta toisaalta yhden-



Kuva 17 ”Kuinka vaikeana keskimäärin pidätte identiteetin- ja pääsynhallintajärjestelmien käyttöönottamista ja konfigurointia? (1=”helppona”, 5=”vaikeana”)” -kysymyksen vastausjakauma

kään trendin luottamusväli ei jää 4:n yläpuolelle, joten poikkeuksellisen merkittäviä trendejä ei tästä joukosta löydy. Sisäisesti vertailtuna pilvipalvelut ja mobiilit päätelaitteet vaikuttavat vahvimmilta trendeiltä viisikosta, mutta erot ovat hyvin pieniä, joten mitään täsmällistä niistä ei kuitenkaan voida sanoa.

Taulukko 5.3. Monivalintakysymysten vastausten tunnusluvut ja luottamusvälit.

Kysymys	Keskiarvo	Keskipoikkeama	95% luottamusväli
Kuinka vaikeana keskimäärin pidätte identiteetin- ja pääsynhallintajärjestelmien käyttöön ottamista ja konfigurointia? (1=”helppona” - 5=”vaikeana”)	3,95	0,92	3,95 ± 0,36
Kuinka paljon seuraavat identiteetin- ja pääsynhallinnan osat tai toiminallisuudet kaipaavat parannusta? (1=”ei lainkaan” – 5=”paljon”)			
Provisiointi	3,29	1,35	3,29 ± 0,53
Federointi	3,25	1,16	3,25 ± 0,47
Hakemistopalvelut	2,05	0,97	2,05 ± 0,38
Deprovisiointi	3,10	1,14	3,10 ± 0,45
Todentaminen	2,71	1,45	2,71 ± 0,57
Valtuuttaminen	3,29	1,23	3,29 ± 0,48
Monitorointi	3,76	1,22	3,76 ± 0,48
Raportointi	3,86	1,01	3,86 ± 0,40
Käytettävyys loppukäyttäjille	4,00	1,00	4,00 ± 0,39
Delegoitu hallinnointi ja itsepalvelu	3,76	1,14	3,76 ± 0,45
Politiikkojen hallinnointi	3,25	1,12	3,25 ± 0,38
Roolienhallinta	3,57	0,98	3,57 ± 0,45
Tehtävien eriyttäminen	3,43	1,33	3,43 ± 0,52
Kuinka paljon uskotte seuraavien trendien vaikuttavan identiteetin- ja pääsynhallintaan? (1=”ei lainkaan” – 5=”paljon”			
Pilvipalvelut	4,05	1,00	4,05 ± 0,39
Mobiilit päätelaitteet (teknisestä näkökulmasta)	4,05	0,95	4,05 ± 0,37
Käyttäjäkeskeiyys	3,67	1,15	3,67 ± 0,45
Bring Your Own Device -käytännöt (sekä politiikka- että turvallisuus-näkökulmasta)	3,73	1,20	3,73 ± 0,46
Kontekstisidonnainen identiteetinhallinta	3,90	0,83	3,90 ± 0,33

5.3 Avoimien kysymysten vastaukset

Kyselyyn sisältyi monivalintakysymysten lisäksi myös avoimia kysymyksiä, joiden tarkoitus oli täydentää monivalintakysymyksiä sekä antaa myös kysymyksen muotoilun ulkopuolista uutta sisältöä. Avoimien kysymysten analysoinnissa vastauksista poimittiin eri vastauksissa esiintyviä aihepiirejä, jotka ovat listattuna frekvenssijärjestyksessä taulukossa 5.4. Kuten luvun 5 alussa kerrottiin, avoimilla kysymyksillä oli tarkoitus saada kerättyä ohjailematonta ja sillä tapaa mahdollisesti arvokasta tietoa asiantuntijoilta sekä selvittää, mitkä asiat tulevat luonnollisesti esille useimmiten. Lisäksi niitä voidaan vertailla soveltuvilta osiltaan monivalintakysymyksistä saatuihin tuloksiin ja selvittää, tukevatko ne niitä vai ilmeneekö jotain ristiriitaa, joka voi syntyä monivalintakysymysten suljetusta luonteesta.

Aihepiirien yhdistelyä edellyttävässä tulkinnassa on pyritty käyttämään hienojakoista erottelua, vaikka vastausten vertailu vaatiikin aina jonkin verran merkityksellistä tulkintaa eri tavalla ilmaistujen mutta samaa tarkoittavien asioiden välillä. Esimerkkinä hienojakoisuudesta toimii heti ensimmäinen kysymys, jonka vastauksissa on eroteltu pääsynhallinta ja todennus, vaikka todennus onkin osa pääsynhallintaa. Erottelu perustuu tässä tapauksessa siihen, ettei todennuksen hyvää toimivuutta voida näillä tiedoilla yleistää koko pääsynhallinnan toimivuuteen, joten erottelu pitää tulokset tarkempina. Lisäksi tarkemmista tuloksista voidaan vähällä vaivalla aggregoida suurempia kokonaisuuksia jos näin halutaan myöhemmin tehdä, mutta sama ei olisi mahdollista toiseen suuntaan. Kysymysten hyvin avoin luonne teki kuitenkin vastauksista hyvin hajanaisia ja jakautuneita, mutta yhtäläisyyksiä ilmeni joidenkin kysymysten välillä yllättävän hyvin tästä huolimatta. Taulukkoon 5.4 on kerätty jokainen aihepiiri, joka toistui vähintään kahdessa eri vastauksessa. Seuraavaksi jokaista kysymystä käsitellään erikseen ja taulukkoon kerättyjen vastausaihepiirien lisäksi listataan suorina lainauksina myös muutama kattava tai muuten hyviä näkökulmia sisältävä vastaus.

Identiteetin- ja pääsynhallintateknologian vahvuudet

Ensimmäisessä kysymyksessä kysyttiin identiteetin- ja pääsynhallintateknologian vahvuuksia ja siitä saatiin kaikista eniten yhteisiä aihepiirejä vastausten välillä. Elinkaarenhallinta, pääsynhallinta ja provisiointi mainittiin kaikkein useimmin, mikä vaikuttaa teknologisessa mielessä positiiviselta, koska ne ovat kaikki identiteetin- ja pääsynhallinnan kannalta hyvin keskeisiä. Provisiointi oli monivalintakysymyksissä epäselvä tapaus, joten tämän voidaan ajatella kallistavan sitä vähemmän parannusta kaipaavaan suuntaan. Seuraavaksi useimmin mainittuina olivat todentaminen, auditointi ja federointi. Todentaminen ja federointi kuuluvat molemmat pääsynhallintaan, joten kokonaisuutena pääsynhallinnan osuus näyttää hyvin edustetulta vahvuuksissa. Monivalintakysymyksissä molemmat olivat epäselviä tapauksia luottamusvälin ylettyessä 3:n molemmin puolin, joten näiden avoimien kysymysten pohjalta on mahdollista, että ne sijoittuisivat todennäköisemmin vähemmän parannusta vaativien ominaisuuksien kategoriaan. Viimeisinä, muttei vähäisimpinä, vahvuuksina tulevat roolienhallinta, identiteettien hallinta, integrointi muihin järjestelmiin, työnkulut sekä raportointi. Sekä roolienhallinta että raportointi olivat monivalintakysymyksissä luokiteltu selvästi parannusta kaipaaviksi, joten jonkinasteista ristiriitaisuutta kysymystyyppien välillä on havaittavissa. Integroituminenkin on hieman ristiriidassa monivalintakysymyksissä haastavaksi havaitun identiteetin- ja pääsynhallintajärjestelmien käyttöönottamisen kanssa, koska integrointi kohde- ja lähdejärjestelmiin on merkittävä osa sitä.

Lopuksi muutamia suoria lainauksia vahvuuksista:

”Efficiency comapared to manual work; less errors; possibility for complex rules.”

”Identity lifecycle management powered with automated processes, Effective Role management, Seggregation-of-duty and security audit/reports, Single-Sign-On, Support for various ERP integration.”

”Cross-platform, agile workflows (provisioning, approval), development in compliance with laws”

”Automated life cycle management of identities”

Taulukko 5.4. Avoimien kysymysten vastauksissa esiintyneiden aihepiirien frekvenssit.

Kysymys	**Aihepiirin frekvenssi vastauksissa**
Identiteetin- ja pääsynhallintateknologian vahvuudet	
Elinkaarenhallinta	6
Pääsynhallinta	6
Provisiointi	5
Todentaminen	4
Auditointi	3
Federointi	3
Roolienhallinta	2
Identiteettien hallinta	2
Integrointi muihin järjestelmiin	2
Työnkulut	2
Raportointi	2
Identiteetin- ja pääsynhallintateknologian heikkoudet	
Ei integroidu helposti	5
Monimutkaisuus	4
Heikko käytettävyys	2
Standardien puute	2
Toteuttaminen kestää liian kauan	2
Identiteetin- ja pääsynhallintateknologian suurimmat uhat	
Toteuttaminen kestää liian kauan	5
Totettaminen on liian kallista	4
Monimutkaisuus	3
Ihmiset	2
Vaikea muutos organisaatioille	2
Muita toiminallisuuksia, jotka kaipaavat parannusta	
Tuki pilvipalveluille	2
Integrointi olemassa oleviin yrityspalveluihin	2
Muita merkityksellisiä trendejä	
Uudet säädökset ja lait	2
Uhkia trendien kehitykselle	
Muutosvastarinta	3
Yksityisyyshuolet	3
Pilvipalvelujen turvallisuus	2
Kustannukset	2

Identiteetin- ja pääsynhallintateknologian heikkoudet

Toisessa kysymyksessä kysyttiin identiteetin- ja pääsynhallintajärjestelmien heikkouksista. Edellisessä kysymyksessä vahvuutena listattu integroituminen saa päinvastaista valoa tämän kysymyksen vastauksissa, joissa ”ei integroidu helposti” on kaikkein useimmiten mainittu heikkous. Heikkoutena se kuitenkin mainittiin selvästi useammin kuin vahvuutena. Toiseksi useimmin mainittuna heikkoutena heti vaikean integroimisen jälkeen tulee järjestelmien monimutkaisuus. Viimeisinä heikkouksina mainitaan heikko käytettävyys, standardien puute ja toteuttamisen vaatima liian pitkä aika. Käytettävyys oli monivalintakysymyksissä luokiteltu eniten parannusta kaipaavaksi ominaisuudeksi, joten tämä heikkous oli odotettavissa, mutta toisaalta vähemmän edustettuna kuin odotettiin. Vaikeasti toteutettava integroituvuus, monimutkaisuus ja liian pitkä toteutusaika puolestaan vastaavat monivalintakysymysten tulosta järjestelmien käyttöönottamisen ja konfiguroinnin vaikeudesta.

Alla lainattu vastaus käsitteli kysymystä hyvin laajasti ja toi esiin useita taulukkoon 5.4 päätyneitä näkökulmia, kuten heikkoa käytettävyyttä loppukäyttäjälle ja standardoinnin puutetta. Näiden lisäksi vastaus toi esiin hyviä uusia näkökulmia identiteettitiedon omistajuuden ja hallinnoinnin jakautumisen suhteen sekä kokonaisvaltaisen toimintasuunnitelman puutetta yksittäisten pistemäisten työkalujen sijaan, jotka ratkaisevat vain tiettyjä yksittäisiä ongelmia ottamatta huomioon muuta ympäröivää järjestelmää.

”Lack of a thought through blueprint for how the various tools fit together to provide end-to-end business value: there are alot of point tools that solves their own technical issues in a vacuum; but no holistic approach to the entire problem area. Lack of widespread adoption of best practice IAM standards in applications (i.e. how applications consume IAM services and/or standardization on how access control in applications should be handled) Lack of "business" alignment; i.e. user friendly interfaces/GUI:s Lack of governance support; i.e. ability to handle the governance around identities and access; who owns & manages roles, who maintains sets of accesses and the lifecycle around them, who takes ownership of identity data and associated company data”

Identiteetin- ja pääsynhallintateknologian suurimmat uhat

Kolmas kysymys käsitteli identiteetin- ja pääsynhallinnan suurimpia uhkia. Tulosten perusteella uhkien ja heikkouksien välinen linjanveto ei ollut vastaajien kesken yhtenäistä, koska merkittävinä uhkina nähdään samoja aihepiirejä kuin mitä heikkouksissakin oli listattuna. Ensimmäisenä parina ovat toteuttamisen liian pitkä kesto ja liian kova hinta. Näiden jälkeen seuraa monimutkaisuus ja lopuksi ihmiset sekä muutoksen vaikeus organisaatiolle, joka ottaa käyttöön uuden identiteetin- ja pääsynhallintajärjestelmän. Toteuttamisen kesto ja hinta sekä järjestelmien monimutkaisuus alkavat jo kuulostaa tutulta tukien edelleen monivalintakysymyksistä saatuja arvioita käyttöön ottamisen vaikeudesta. Ihmiset-aihepiiri käsitti vastauksissa sekä sisäpiirin uhkia että inhimillisiä uhkia yleisesti aina vahingoista huolimattomuuteen ja tietoiseen, muttei välttämättä pahantahtoiseen sääntöjen kiertämiseen. Muutoksen vaikeus organisaatiolle sen sijaan oli tervetullut huomio, joka tuo esiin identiteetin- ja pääsynhallintaan liittyviä ei-teknologisia haasteita, joita kuitenkin mahdollisesti voitaisiin helpottaa teknologisinkin keinoin.

Alla muutamia suoria lainauksia vastauksista:

”Current solutions are too HEAVY (in cost and time) for most smaller business. Organised crime is the biggest threat”

”Cost brought on by overly complex solutions.”

”'Threats to IAM in general': hard to implement; expensive; major/hard change for many organizations.
'Security threats to IAM solutions': Without proper hardening and security event monitoring, IAM systems open the door to the kingdom.”

Muita toiminnallisuuksia, jotka kaipaavat parannusta

Taulukon neljäs kysymys keskittyi monivalintakysymyksissä parannusta vaativien ominaisuuksien ja toiminnallisuuksien listalta jääneisiin toiminnallisuuksiin, jotka myös vaativat parannusta. Kysymykseen jätettiin usein vastaamatta, minkä vuoksi yhtäläisyydet olivat myös harvassa. Kuitenkin kaksi toiminnallisuutta saivat kaksi mainitsemiskertaa. Nämä olivat eli tuki pilvipalveluille ja aiemminkin tavalla tai toisella mainittu integrointi olemassa oleviin kohde- ja lähdejärjestelmiin.

Seuraavaksi muutamia parannusta kaipaavia asioita, jotka eivät päässeet listalla, vastauksista lainattuina:

”Privileged Identity management, impact simulation, support for cloud environments, Identity Federation”

”Attestation and recertification processes in business terminology. Audit trail security and report readiness.”

”Configuration and code life cycle management. Version control. Package management. Controlled deployment.”

”In IdM, the entity model of the product limits how the organisation defines it's identities and applies processes to them. Allowing a more complex and customisable entity model would allow the IdM solutions to support different business models more flexibly.”

Muita merkityksellisiä trendejä

Viidennessä kysymyksessä kysyttiin kyselyssä mainittujen trendien ulkopuolisia identiteetin- ja pääsynhallinnan kannalta merkityksellisiä trendejä. Kuten neljännessäkin kysymyksessä, vastausprosentti tähän kysymykseen oli pieni. Yksi trendi kuitenkin saatiin esille: uudet lait ja säädökset. Tämä oli erittäin hyvä huomio, sillä etenkin identiteetinhallintaa koskee hyvin vahvasti lait muuan muuassa henkilötietojen käsittelystä, ja mikäli tällaiset lait muuttuvat, ne voivat vaikuttaa hyvin vahvasti sekä identiteetinhallintaan yleisesti että identiteetinhallintateknologian suunnitteluun.

Alla on taas lainattu vastauksia, jotka sisältävät myös jonkin verran lisää trendejä:

”I believe bio-metric authentication (Face, Retina, Finger Print) would be more pervasive in the future owing to its fool-proof nature and this would affect the complexity of the IAM implementations.”

”Claimns based identity management”

”Data proliferation (Big data / explosion of data & information, and the places where information are stored and managed)”

”Due Increasing support of federated identities small and mid-size companies will be less interested in development of their own IdPs and mostly concentrate on access policies.”

Uhkia trendien kehitykselle

Kuudes kysymys käsitteli mahdollisia uhkia monivalintakysymyksissä listatuille trendeille. Kärjessä olivat ihmisten taipumus vastustaa muutosta sekä yksityisyyshuolet, jotka keskittyivät pääosin pilvipalveluihin. Pilvipalvelujen turvallisuus esiintyi myös omana mainintanaan korkeat kustannukset tullessa lähellä perässä. Muutosvastarinnan, yksityisyyshuolien ja pilvipalveluiden turvallisuuden voidaan ajatella kaikkien koskettavan vahvasti pilvipalveluja, jotka muuttavat monia perinteiseen verkko- ja laskentateknologiaan liittyviä perusoletuksia. Nämä perusoletukset koskevat tiedon ja laitteiston hallinnointia ja omistajuutta, mitkä puolestaan johtavat oletuksiin yksityisyydestä ja turvallisuudesta.

”Laws that limit usage/storage of identity information outside of company premises or cross-country personal data transfer”

”Compliance of cloud-based solutions is a barrier (visibility into the cloud)”

”Complexity of business needs, Project life span.”

”Design paradigm of the current major products”

Yleisellä tasolla avoimet kysymykset tukivat hyvin joitain monivalintakysymysten antamia tuloksia ja antoivat myös muutamia uusia näkökulmia, kuten lakien ja säädösten merkityksen sekä uuden identiteetin- ja pääsynhallintajärjestelmän käyttöönoton vaikeuden organisaatiolla. Lisäksi ne toimivat jonkinlaisena suuntaviittana joidenkin monivalintakysymysten vastauksissa epäselviksi jääneiden tapauksien tulkinnassa. Vastauksissa oli paikoittain myös ristiriitaa, sekä sisäisesti että monivalintakysymyksiin verrattuna, mutta usein toinen ristiriitaisista kannoista oli selvässä vähemmistössä suhteessa toiseen.

5.4 Kyselyn toteutuksen analyysi

Tässä luvussa käsitellään kyselyn toteuttamiseen liittyviä haasteita. Tällaisia haasteita ovat muun muassa ongelmat ja havaitut heikkoudet, jotka liittyvät yleensä joko kyselyn suunnitteluun tai jakelun toteutukseen. Näille ongelmille esitetään myös mahdollisia parannusehdotuksia tulevaisuuden varalta.

Kyselyn suurin ongelma oli vastausten vähäinen määrä ja sen aiheuttama heikentynyt tulosten käyttökelpoisuus muun muassa luottamusvälien leventymisen vuoksi. Selvä haaste perusjoukon suhteen oli se, että kyseessä olivat tietyn erikoisalan asiantuntijat, joita on moniin muihin perusjoukkoihin verrattuna hyvin vähän. Esimerkiksi 100:n vastauksen saaminen, mikä olisi hyvä pohja kvantitatiiviselle analyysille, tällaiselta perusjoukolta on varsin haastavaa. Tämä on kuitenkin asia, joka ei ole muutettavissa, joten vastausprosentin kasvattamiseen on keksittävä jatkossa jotain muuta. Seuraavaksi analysoidaan eri jakelukanavia tehokkuuden suhteen.

- *Yrityksien lähestyminen suoraan sähköpostilla* oli kaikista tehottominta suhteessa käytettyyn aikaan. Ajankäyttöä lisäsi sähköpostipohjien laatiminen sekä suomeksi että englanniksi ja kohdeyritysten sekä niiden sähköpostiosoitteiden etsiminen. Vastauksia saatiin vain yksi useista kymmenistä lähetetyistä

- *Henkilökohtaiset kontaktit* toimivat hyvin ja niissä vastausprosentti oli yli 50%. Käytettävä kontaktiverkosto ei kuitenkaan ollut tarpeeksi laaja, jotta sillä olisi saatu likimainkaan tarvittavaa määrää vastauksia. Ajankäytöllisesti sähköpostien kirjoittaminen on tässäkin jakelutavassa edelleen melko tehotonta.

- *Verkostoitumissivuston ammattialan ryhmiin kirjoittaminen* oli jakelutavoista kaikista tehokkainta ja tuotti yli kolme neljännestä saaduista vastauksista kaikista vähimmällä vaivalla. Tämä jakelutapa tavoitti myös selkeästi suurimman ja globaalimman vastaajakunnan, joten tulevaisuuden kannalta vastaavassa tapauksessa se olisi ensimmäinen ja pääasiallinen valinta.

Vastaushävikkiä olisi voitu yrittää pienentää myös motivoimalla vastaajia jollain pienellä arvottavalla palkinnolla, esimerkiksi lahjakortilla. Tätä lähestymistapaa harkittiin tutkimusta toteutettaessa, mutta sen ei arveltu olevan tarpeellista ja toisekseen sitä pidettiin ylimääräisenä kustannuksena. Lisäksi oli pelättiin, että henkilöt, jotka eivät aidosti olisi alan ammattilaisia vastaisivat kyselyyn vain palkinnon toivossa. Jälkikäteen ajatellen, jos jakelukanavina käytettäisiin verkostoitumissivuston ryhmiä ja vastauksia saataisiin runsaasti, mahdolliset huijarit hukkuisivat tilastoihin ja pelko jäisi näin ollen melko turhaksi suhteessa saavutettuun hyötyyn. Kustannuksetkaan tuskin olisivat lopulta liian suuret.

Vastaushävikin lisäksi avoimien kysymysten vastaukset olivat hyvin hajanaisia ja niistä oli vaikeaa tehdä varsinaisia johtopäätöksiä. Trendejä olisi voinut ilmetä helpommin suuremmalla vastausmäärällä, mutta enemmän ongelmana vaikutti kuitenkin olevan kysymysten liian avoin luonne. Vaikka idea siitä, että ihmiset vastaisivat täysin johdattelemattomasti ja tällaisia ”ensimmäisinä päähän tulevia” ajatuksia saataisiin kerättyä ja yhdisteltyä, on lähtökohtaisesti hyvä, olisi rajaus voinut olla kuitenkin hieman täsmällisempää. Monissa avoimissa kysymyksissä pystyi valitsemaan sekä teknologialähtöisen että ei-teknologisen näkökulman asiaan, jotka hajauttivat selvästi vastauksia. Erilliset kysymykset eri näkökulmille olisivat todennäköisesti tuottaneet paremmin analysoitavia tuloksia. Tulkinnanvara ilmeni jopa henkilötietojen keräyskysymyksissä, missä ”alan kokemus” -kysymyksessä olisi ollut hyvä olla vuosimäärä sulkeissa täsmentämään, että yleisen kuvauksen lisäksi toivottiin vuosiarviota kokemuksesta, koska useat vastaajat jättivät vuosimäärän ilmoittamatta.

Viimeisenä, mutta keskeisenä, heikkoutena oli aika, joka vastausten keräämiseen oli varattu. Nyt kysely oli saatavilla vain kaksi kuukautta ja tästä yli ensimmäisen puoliskon tästä se oli vain tehottomien jakelutapojen varassa. Jos kysely olisi tehty ja laitettu levitykseen esimerkiksi neljä kuukautta aikaisemmin ja käyttäen hyväksi havaittua jakelutapaa, niin saatujen vastausten määrän voitaisiin arvella olevan kaksin- tai jopa kolminkertainen ilman mitään lisämotivaattoriakin.

Kyselyn jälkeen on muodostunut selkeästi parempi kuva siitä, miten kysely kannattaisi järjestää jatkossa vastaavantyyppisessä tapauksessa. Kyselylle tulisi valita oikea jakelukanava, varata riittävästi aikaa ja tarvittaessa motivoida vastaajia palkinnolla. Heikkouksistaan huolimatta tämäkin kysely onnistui tuottamaan joitakin käyttökelpoista tuloksia ja mielenkiintoista tietoa.

5.5 Yhteenveto

Kyselyyn osallistui lopulta 22 asiantuntijaa, joten vastausmäärä jäi toivottua vähäisemmäksi, mikä teki johtopäätöksien tekemisestä joidenkin kysymysten osalta vaikeaa. Toisaalta osasta vastauksia pystyttiin tekemään tästä huolimatta joitain kiinnostavia johtopäätöksiä. Kiinnostavia tuloksia saatiin paitsi monivalintakysymysten myös avoimista kysymysten vastauksista tehdyn vertailun ja analyysin pohjalta.

Ensimmäisen monivalintakysymyksen pohjalta identiteetin- ja pääsynhallintajärjestelmien käyttöönoton ja konfiguroinnin vaikeuden keskimääräinen arvio oli 3,95 ± 0,36 95%:n luottamusvälillä, joka oli merkittävästi yli keskimääräisen vaikeuden (3, asteikolla 1–5). Tämän pohjalta ainakin järjestelmien valmistajien olisi perustellusti syytä panostaa käyttöönoton ja konfiguroinnin helpottamiseen. Avoimien kysymysten vastausten puolelta saatiin muitakin yleisiä parannuksen aiheita, sillä suurimmiksi heikkouksiksi oli vastausten kesken useimmiten mainittuina järjestelmien vaikea integroiminen ja monimutkaisuus. Suurimpina uhkina mainittiin samansuuntaisesti toteuttamisen pitkä kesto ja korkeat kustannukset sekä monimutkaisuus. Vastauksissa oli myös integroitumisen suhteen hieman ristiriitaa, koska se oli listattu vahvuuksienkin puolella avoimissa kysymyksissä, mutta sen edustus vahvuutena oli kuitenkin selvästi vähäisempi kuin heikkouden osalta. Monivalintakysymyksissä olleiden osa-alueiden lisäksi avoimien kysymysten pohjalta parannusta kaipaaviin osa-alueisiin voidaan lisätä myös tuki pilvipalveluille.

Muita monivalintakysymysten tuloksista paljastuneita 95%:n luottamusvälillä merkittävää parannusta kaipaavia identiteetin- ja pääsynhallintateknologian osa-alueita olivat käytettävyys (4,00 ± 0,39), raportointi (3,76 ± 0,48), monitorointi (3,76 ± 0,48), delegoitu hallinnointi ja itsepalvelu (3,76 ± 0,45) sekä roolienhallinta (3,57 ± 0,45). Avoimien kysymysten vastauksista saadut tulokset teknologian heikkouksista tukivat myös käytettävyyden heikkoa tilaa. Raportoinnin osalta avoimien kysymysten vastaukset olivat puolestaan ristiriidassa monivalintakysymysten tulosten kanssa, koska niissä raportointi oli listattu vahvuutena. Toisaalta sen edustus vahvuutena oli vähäinen, joten tästä ristiriidasta huolimatta voidaan sanoa, että kappaleen alussa mainitut osa-alueet todella kaipaavat merkittävää parannusta. Nämä havainnot voivat aiempien ohella auttaa valmistajia kohdentamaan paremmin tuotteidensa kehitystä ja keskittymään entistä tehokkaampien heikkouksien korjaamiseen.

Parannusta kaipaavien osa-alueiden ohella selvisi monivalintakysymyksissä myös yksi osa-alue, johon oltiin yleisesti hyvin tyytyväisiä. Hakemistopalvelut perustuvat verrattain vanhaan teknologiaan, mutta se sai keskimääräiseksi arviokseen 2,05 ± 0,38 eli merkittävästi alle kolmen. Tämän pohjalta hakemistopalveluiden kehitys voidaan perustellusti sijoittaa identiteetin- ja pääsynhallintajärjestelmien kehitysprioriteettilistan hännille. Avoimien kysymysten osalta useimmiten mainittujen vahvuuksien kärjessä olivat elinkaarenhallinta, pääsynhallinta, provisiointi ja todentaminen. Näiden havaintojen pohjalta provisiointia (ja mahdollisesti myös deprovisiointia) sekä todentamista voitaisiin siirtää kypsempien, ei merkittävää parannusta kaipaavien toiminnallisuuksien kategoriaan.

Muiden toiminnallisuuksien osalta ei saatu niin tarkkoja tuloksia, että niistä voitaisiin hyvällä varmuudella sanoa mitään suuntaan tai toiseen - niiden kaikkien luottamusvälit ylettyivät kolmen molemmin puolin.

Identiteetin- ja pääsynhallintateknologiaan vaikuttavien trendien osalta ei ilmennyt mitään yllättävää, vaan kaikki monivalintakysymyksissä mukana olleet trendit kategorisoituivat merkittäväksi trendeiksi. Asteikolla 1–5 vaikutuksen merkityksellisyyden kärjessä olivat pilvipalvelut (4,05 ± 0,39) ja mobiililaitteet (4,05 ± 0,37), pian niiden perässä kontekstisidonnainen identiteetinhallinta (3,90 ± 0,33) ja listan hännillä Bring Your Own Device -käytännöt (3,73 ± 0,46) sekä käyttäjäkeskeisyys (3,67 ± 0,45). Avoimissa kysymyksissä tuli mukaan yksi useammin kuin kerran mainittu trendi lisää eli uudet lait ja säädökset. Tätä trendiä voidaan pitää hyvin merkityksellisenä, koska varsinkin identiteetinhallinta sisältää paljon henkilötietojen käsittelyä, joka on vahvasti laeilla ja direktiiveillä säädeltyä. Kaiken kaikkiaan kaikkien kyselyssä mainittujen trendien voidaan tulosten perusteella odottaa vaikuttavan identiteetin- ja pääsynhallinnan kehitykseen tulevaisuudessa.

6 Identiteetinhallintajärjestelmien tulevaisuuden näkymät: pilvipalvelut

Tämä luku kertoo luvussa 5 esiteltyjen asiantuntijakyselyn tulosten perusteella valitusta identiteetin- ja pääsynhallintaan hyvin merkittävästi vaikuttavasta trendistä eli pilvipalveluista. Tässä luvussa avataan ensin pilvipalvelun käsitettä ja sitten siirrytään käsittelemään pilvien palvelu- ja sijoitusmalleja. Tämän pohjustuksen jälkeen käsitellään vielä pilvipalvelujen hyötyjä ja haasteita identiteetinhallinnan kannalta sekä identiteetinhallintaa pilvipalveluna.

6.1 Pilvipalvelut

Pilvilaskennalla (engl. cloud computing) tarkoitetaan verkkopohjaista tietokoneen käyttöä, jossa ryhmä etäpalvelimia hoitaa kaiken tiedon tallentamisen, hallinnan ja laskennan paikallisen palvelimen tai käyttäjän tietokoneen sijasta [49]. Termillä pilvilaskenta viitataan sekä niihin sovelluksiin, joita tarjotaan palveluna verkon yli, että niihin sovelluksiin ja laitteistoon, joiden päällä nämä palvelut ajetaan [50, s. 50]. Itse pilvi on terminä yksinkertaistettu kuvaus samaan tapaan kuin Internet, joka abstrahoi kaikki monimutkaiset laitteiden väliset yhteydet ja suhteet, joista maailmanlaajuinen verkko todellisuudessa rakentuu. [51, s. 23]

Mather et al. määrittelevät pilvilaskennan siten, että se perustuu viidelle peruspiirteelle: monivuokralaisuudelle (engl. multitenancy), suurelle skaalautuvuudelle, joustavuudelle (engl. elasticity), käyttöpohjaiselle maksamismallille (engl. pay as you go) ja resurssien provisioinnille itsepalveluna [51, s. 7]. Nämä peruspiirteet on selitetty lyhyesti alla:

- *Monivuokralaisuus* tarkoittaa sitä, että toisin kuin perinteisissä laskentamalleissa, jotka olettivat laskentaresurssien olevan täysin omistetut, pilvilaskenta perustuu mallille, jossa laskentaresurssit ovat jaettuja. Tämä tarkoittaa esimerkiksi sitä, että samaa resurssia voi käyttää samanaikaisesti monet käyttäjät verkko-, palvelin- tai jopa sovellustasolla. [51, s. 7]

- *Suuri skaalautuvuus* tarkoittaa sitä, että vaikka yksittäisillä organisaatioilla voi olla satoja tai jopa tuhansia järjestelmiä, mahdollistaa pilvilaskenta skaalautumisen ainakin kymmenien tuhansien järjestelmien kertaluokkaan. Lisäksi sen kyky skaalata muun muassa verkon kaistanleveyttä tai tallennustilaa on niin ikään hyvin suuri. [51, s. 7]

- *Joustavuus* tarkoittaa sitä, että käyttäjät voivat nostaa ja laskea käyttämiensä laskentaresurssien määrää tarpeen mukaan. Mikäli käyttäjät eivät enää lainkaan tarvitse jotain resurssia, he voivat vapauttaa sen kokonaisuudessaan muihin tarkoituksiin. [51, s. 7]

- *Käytön mukainen maksamismalli* tarkoittaa, että käyttäjät maksavat vain käyttämistään resursseista ja vain siitä ajasta, jonka ne ovat niitä käyttäneet. [51, s. 7]

- *Resurssien provisiointi itsepalveluna* tarkoittaa, että käyttäjät voivat provisioida uusia järjestelmiä, kuten laskentatehoa, sovelluksia ja tallennustilaa, sekä verkkoresursseja itsepalveluna ilman kenenkään panosta palveluntarjoajalta [51, s. 7][52, s. 2].

Amerikkalainen teknologian standardointielin National Institute of Standards and Technology (NIST) tarjoaa toisen tulkinnan pilvilaskennan ominaispiirteille, joita on niin ikään viisi. Ne ovat tarpeenmukainen itsepalvelu (engl. on-demand self-service), laaja pääsy verkon kautta (engl. broad network access), resurssien yhdistäminen (egl. resource pooling), nopea joustavuus (engl. rapid elasticity) ja mitattu palvelu (engl. measured service): [52, s. 2]

- *Tarpeenmukaisella itsepalvelulla* käyttäjä voi yksipuoleisesti provisioida laskentaresursseja, kuten palvelinaikaa ja verkkotallennustilaa, aina tarpeen mukaan ilman, että kenenkään palveluntarjoajan puolelta tarvitsisi tehdä mitään asian eteen. [52, s. 2]

- *Laajalla pääsyllä verkon kautta* tarkoitetaan palvelujen tarjoamista verkon kautta sellaisilla standardoiduilla mekanismeilla, jotka mahdollistavat käytön monimuotoisilla käyttäjäalustoilla kuten älypuhelimilla, taulutietokokeilla, kannettavilla tietokoneilla ja työasemilla. [52, s. 2]

- *Resurssien yhdistäminen* tarkoittaa, että pilvipalveluntarjoajan laskentaresurssit on kerätty yhteiseen pooliin, josta niitä voidaan jakaa useille asiakkailla niiden tarpeiden mukaisesti. Nämä fyysiset ja virtuaaliset resurssit, kuten laskentateho, muisti, tallennustila tai kaistanleveys, voidaan myöntää ja uudelleen kohdentaa dynaamisesti tarpeiden muuttuessa. Asiakas ei voi varsinaisesti tarkkaan tietää saati vaikuttaa, missä laskenta tapahtuu paitsi ehkä korkean tason abstraktioilla, kuten maa- tai konesalivalinnalla. [52, s. 2]

- *Nopealla joustavuudella* tarkoitetaan sitä, että järjestelmän resursseja voidaan joustavasti provisioida ja vapauttaa nopeasti vastaamaan asiakkaiden tarpeita. Asiakkaan näkökulmasta käyttöön provisioitavat resurssit voivat vaikuttaa lähes rajattomilta ja niitä voidaan ottaa käyttöön milloin vain ja missä suurusluokassa tahansa. [52, s. 2]

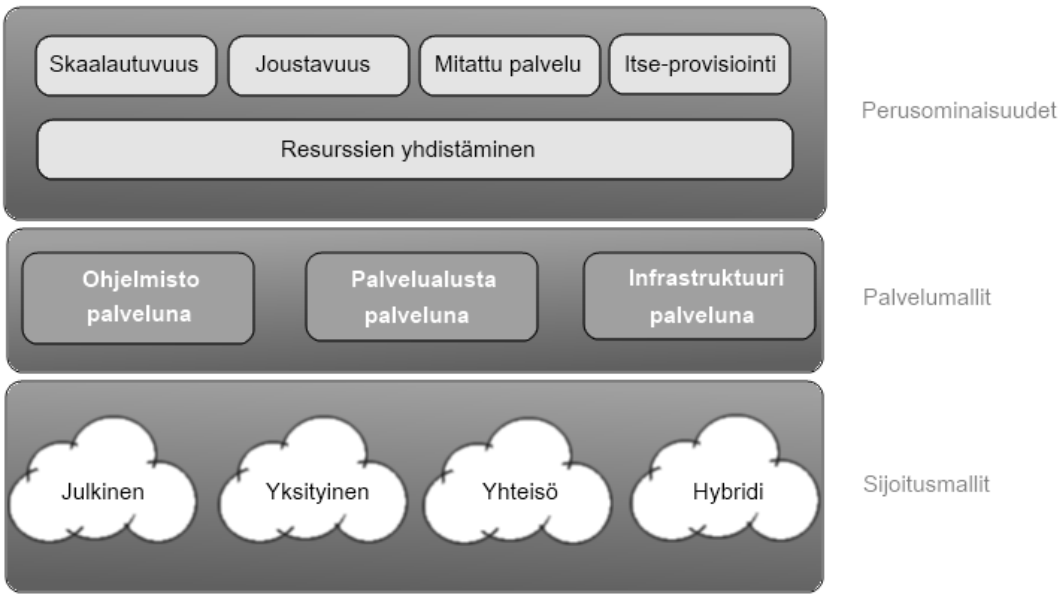
- *Mitattu palvelu* tarkoittaa pilvipalvelun kykyä automaattisesti säädellä ja optimoida resurssien käyttöä mittaamalla kullekin palveluille ominaista resurssien kulutusta. Mitattavat resurssit voivat olla muun muassa laskentatehoa, tallennustilaa, kaistanleveyttä tai aktiivisia käyttäjätilejä, ja toimivat pohjana laskutukselle. Resurssien käyttöä voidaan myös tarkkailla ja raportoida, mikä tuo läpinäkyvyyttä käyttömääriin sekä palvelun tarjoajalle että sen asiakkaille. [52, s. 2]

Molemmat tulkinnat näyttävät tuovan suoraan esiin itsepalveluna provisioitavien resurssien sekä joustavuuden että resurssien kohdentamisen. Kuvauksien perusteella myös monivuokralaisuus ja resurssien yhdisteleminen sekä käytönmukainen maksamismalli ja mitattu palvelu käsittelevät hyvin samankaltaisia vaatimuksia. Sen sijaan annettujen määritelmien perusteella on vaikeampi löytää suoraa vastinetta skaalautuvuudelle ja laajalle pääsylle. Tietyllä tapaa laaja pääsykin käsittelee skaalautuvuutta, koska palvelu skaalautuu eri alustoille ja laitteille. Kuitenkin tämä on erilaista skaa-

lautuvuutta kuin ensimmäisessä määritelmässä, jossa puhutaan vain käyttäjien lukumäärän sitä kautta aiheutuvien resurssien kulutuksen mukana skaalautuvuudesta. Toisaalta voidaan myös ajatella, että tukemalla laajaa skaalaa laitteita ja alustoja käyttäjäkunta voi kasvaa. Tämä viittaa implisiittisesti siihen, että järjestelmän on skaalauduttava myös käyttäjämäärien mukaan. Lopulta tämä on kuitenkin määritelmien ulkopuolista spekulaatiota. Lopulta voidaan vain todeta, että tulkinnat ovat suurelta osin yhtenevät ja niiden eroavia osia voidaan käsitellä erikseen aina kun käsiteltävä aihe sitä edellyttää.

Virtualisointi on pilvilaskennan kannalta keskeinen käsite, jolla tarkoitetaan yksinkertaistettua kuvausta varsinaisista laskentaresursseista, kuten prosessoinnista, tallennustilasta, muistista ja verkkoyhteyksistä, sovelluksia ja asiakkaita varten. Se mahdollistaa pilvipalveluiden monivuokralaisuuden tarjoamalla kaikille asiakkaille jaetun ja skaalautuvan resurssipohjan, joka kuitenkin näkyy jokaiselle asiakkaalle perinteisinä täysin omistettuina resursseina. [51, s. 14] Näin jokainen asiakas saa esimerkiksi oman virtuaalisen palvelimen, käyttöjärjestelmän tai sovelluksen käyttöönsä, vaikka tämä virtuaalinen instanssi saa todelliset resurssinsa samasta jaetusta poolista kuin kaikkien muidenkin asiakkaiden virtuaaliset instanssit. Näiden virtuaalisten resurssiinstanssien ja todellisten resurssien rajapintaa hoitaa erityinen virtuaalikoneiden hallintayksikkö, hypervisor [51, s. 14]. Se on suoraan fyysisen laitteiston päällä ajettava pieni sovellus, joka implementoi ja hallinnoi virtuaalikoneiden käyttämät virtuaaliset prosessorit, muistin ja muut tarvittavat komponentit sekä kaiken tiedon siirtämisen ja signaloinnin näiden komponenttien välillä [51, s. 14].

Pilvilaskennalla toteutettuja palvelukokonaisuuksia kutsutaan pilvipalveluiksi ja tätä termiä tullaan käyttämään tässä luvussa laajemmin käsittämään myös itse pilvilaskennan. Pilvipalvelut voidaan jakaa pilvilaskennan omaispiirteisiin, palvelumalleihin ja sijoitusmalleihin [52, s. 2]. Kaikkien pilvipalvelujen tulisi määritelmän täyttää ainakin suurin osa pilvilaskennan ominaispiirteistä, mutta palvelumallit ja sijoitusmallit tarjoavat enemmän vaihtelua. Kolme yleisintä pilvipalvelumallia ovat palveluna tarjottava ohjelmisto (engl. Software as a Service, SaaS), palveluna tarjottava palvelualusta (engl. Platform as a Service, PaaS) ja palveluna tarjottava infrastruktuuri (engl. Infrastructure as a Service). Yleisimmät sijoitusmallit taas ovat julkinen pilvi, yksityinen



Kuva 18: Pilvimallin rakenne [53, kuva 1, piirretty uudestaan]

pilvi, yhteisöpilvi (engl. community cloud) ja hybridipilvi (engl. hybrid cloud). Tätä pilvipalvelun mallia on havainnollistettu kuvassa 18.

6.2 Pilvien palvelumallit

Pilvipalvelu voidaan tarjota asiakkaalle eri teknologiakerroksina: ohjelmistona, alustana tai infrastruktuurina. Tarjottavan kerroksen valinta vaikuttaa asiakkaan palvelusta saamiin hyötyihin, vaikutusmahdollisuuksiin sekä vastuisiin. Näitä eri kerroksina tarjottavia palvelumalleja ja niiden ominaisuuksia käsitellään seuraavaksi.

Palveluna tarjottava ohjelmisto (SaaS)

Palveluna tarjottava ohjelmisto mahdollistaa pilvipalveluntarjoajan tarjoamien sovellusten ajamisen pilvi-infrastruktuurissa [52, s. 15]. Toisin kuin perinteisessä ohjelmistojen ostomallissa, asiakas ei varsinaisesti osta ohjelmistoa, vaan vuokraa sitä pilvipalveluntarjoajalta. Tämä tarkoittaa asiakkaan kustannuksien muuttumista pääomakustannuksista, jotka perinteisessä mallissa liittyvät ohjelmistolisenssien ja laitteiston ostoon, operaatiokustannuksiin jotka käsittävät vain sovelluksen käytöstä koituvat kustannukset. [51, s. 18] Esimerkkejä palveluna tarjottavasta ohjelmistosta ovat muun muassa yksityisille käyttäjillekin tarjottava sähköpostipalvelu Google Mail ja yrityksille suunnattu asiakassuhteidenhallintapalvelu Salesforce.com.

Koska sovellukset ajetaan pilvi-infrastruktuurissa eikä päätelaitteilla, niitä ei tarvitse erikseen ladata ja asentaa jokaiselle laitteelle. Niitä voidaan ajaa erilaisten rajapintojen kautta, esimerkiksi pelkällä internetselaimella tai sitten jollain tarkemmin rajatulla pääteohjelmarajapinnalla. [51, s. 18] Sovelluksen ajaminen pilvessä mahdollistaa myös sovelluksen käytön hyvin eritasoisilla päätelaitteilla [51, s. 18], kuten esimerkiksi älypuhelimilla, koska kaikki raskas prosessointi tapahtuu palveluntarjoajan infrastruktuurissa päätelaitteen sijaan.

Palveluna tarjottavat ohjelmistot on yleensä sijoitettu julkiseen pilveen [51, s. 18], koska siten ne voivat hyötyä eniten pilvipalvelun monivuokralaisuusominaisuudesta. Monivuokralaisuus mahdollistaa laajan asiakaskunnan ja sen myötä suuremman rahavirran. Asiakkaan näkökulmasta monivuokralaisuus madaltaa yleensä palvelun hintaa, mutta voi tuoda toisaalta mukanaan myös huolen tietojen vuotamisesta muille asiakkaille. Tämän takia pilvipalveluntarjoajat pyrkivätkin varmistamaan, että vaikka palveluna tarjottavassa ohjelmistossa kaikki asiakkaat jakavatkin saman fyysisen laitteistoinfrastruktuurin, jokainen on silti loogisesti eroteltu eikä muilla asiakkailla ole näkyvyyttä toisten toimiin [51, s. 19].

Palveluna tarjottava palvelualusta (PaaS)

Palveluna tarjottava palvelualusta on palveluna tarjottavaa ohjelmistoa laajempi kokonaisuus. Se tarjoaa asiakkaalle kokonaisen kehitysympäristön, jossa tämä voi kehittää ja tarjota omia palvelujaan. Palveluiden kehitys tapahtuu yleensä pilvipalveluntarjoajan toimittamilla kehitystyökaluilla ja esiohjelmoiduilla palikoilla, joista asiakkaat rakentavat omat palvelunsa. Näiden esiohjelmoitujen palikoiden käyttö tekee sovelluskehittämisestä mahdollisen myös ilman erikoistuneita ohjelmointitaitoja, kuten Java- tai JavaScript-osaamista, mikä tarkoittaa että merkittävästi suurempi määrä ihmisiä pystyy tekemään kehitystyötä. [51, s. 19] Esimerkkeinä palveluna tarjottavista palvelualustoista ovat muun muassa Windows Azure ja Google AppEngine.

Palveluna tarjottavat palvelualustat mahdollistavat yksinkertaisen tavan suunnitella ja perustaa verkkopalveluja ilman niitä kustannuksia ja sitä vaivaa, mitä omien palvelimien ostaminen ja konfigurointi vaatisi. Sovellusten kehitystyökalut sijaitsevat pilvessä ja niitä voidaan käyttää pelkällä internetselaimella ilman, että kehittäjien tarvitsisi asentaa mitään sovelluksia työasemilleen. [51, s. 20]

Palveluna tarjottava infrastruktuuri (IaaS)

Palveluna tarjottava infrastruktuuri on palvelualustaakin laajempi palvelukokonaisuus, jossa asiakas vuokraa tai ostaa kokonaisen infrastruktuurin, jolla pyörittää haluamiaan sovelluksia. Tämä kokonaisuus sisältää yleensä omistetun laitteistoinfrastruktuurin sekä ohjelmistoinfrastruktuurin, joka voi pilvilaskentaperiaatteiden mukaisesti skaalautua kysynnän mukaan. Skaalautuminen voi olla sekä lyhytaikaista, jonka tarkoitus on vain vastata hetkellisiin kulutuspiikkeihin, että pitkäaikaista kapasiteetin lisäystä kokonaiskysynnän kasvaessa. [51, s. 22] Esimerkkeinä palveluna tarjottavista infrastruktuureista toimivat muun muassa Amazon Webservices ja Google Compute Engine.

6.3 Pilvien sijoitusmallit

Pilvien sijoitusmallit kuvaavat sitä, miten eri pilvipalvelut on toteutettu ja minne ne on sijoitettu verkossa. Yleisimmät sijoitusmallit ovat julkinen pilvi, yksityinen pilvi, yhteisöpilvi sekä hybridipilvi. [51, s. 23].

Julkiset pilvet

Julkiset pilvet kuvaavat pilvilaskentaa perinteisessä mielessä, jossa resursseja provisioidaan hienojakoisella itsepalveluperusteella Internetin yli. Pilvipalveluntarjoaja on tällöin kolmas osapuoli, joka hoitaa resurssien jakamisen ja laskuttaa tarkasti käytettyjen resurssien pohjalta. [51, s. 23]

Julkisten pilvien infrastruktuuri on tarkoitettu provisioitavaksi avoimesti kaikelle yleisölle. Sen voi omistaa yritys, akateeminen instituutio, jokin valtion organisaatio tai jokin yhdistelmä näistä. [52, s. 3] Nämä organisaatiot vastaavat pilven yleisestä hallinnasta ja turvallisuudesta, eikä asiakkaalla tästä syystä ole paljoa valtaa vaikuttaa pilvipalvelun fyysisiin tai loogisiin turvallisuusaspekteihin. [51, s. 23]

Yksityiset pilvet

Yksityiset pilvet on sijoitettu yksityiseen verkkoon, ja niiden tarkoitus on palvella ainoastaan pilven omistajaorganisaatiota. Ne eivät täten ole monivuokralaispalveluja, kuten muut pilvityypit. Organisaatiot voivat rakentaa ja hallinnoida yksityiset pilvipalvelunsa itse, mutta tämä tarkoittaa sitä, etteivät ne voi hyötyä julkisen pilven tapaan alemmista pääoma- ja hallinnointikustannuksista. [51, s. 23] Vaihtoehtoisesti organisaatiot voivat myös ulkoistaa pilvipalvelun rakentamiseen ja ylläpitoon liittyviä tehtäviä osittain tai kokonaan kolmannelle osapuolelle, kuten kuva 19 havainnollistaa.

Yhteisöpilvi

Yhteisöpilvet muistuttavat yksityisiä pilviä sillä erotuksella, että sen palvelut on tarkoitettu yhteisön käyttöön yksittäisen organisaation sijasta. Yhteisöt koostuvat yleensä organisaatioista, joilla on yhteisiä intressejä toiminnan, turvallisuusvaatimusten tai muiden tekijöiden suhteen. Sen omistajuus ja hallinnointivastuu voi olla jollain yksittäisellä yhteisön organisaatiolla, niillä kaikilla, jollain kolmannella osapuolella tai millä tahansa yhdistelmällä näistä. [52, s. 3] Koska yhteisöpilvi jaetaan usean organisaation kesken, se tulee yksittäiselle organisaatiolle halvemmaksi toteuttaa ja hallinnoida kuin yksityinen pilvi.

Hybridipilvi

Hybridipilvi koostuu useista eri pilvipalveluntarjoajista, jotka voivat olla sekä sisäisiä että ulkoisia. Organisaatio voi esimerkiksi ajaa ei-kriittisiä sovelluksia julkisessa pilvessä, mutta pitää kriittiset sovellukset ja sensitiivisen tiedon sisäisessä, yksityisessä, pilvessä. [51, s. 25] Hybridipilvi on siis nimensä mukaisesti yhdistelmä julkisia ja yksityisiä pilviä.

	Infrastruktuuria hallinnoi	Infrastrukuurin omistaa	Infrastruktuurin sijoituspaikka	Käyttäjät
Julkinen	Kolmas osapuoli	Kolmas osapuoli	Organisaation tilojen ulkopuolella	Ei-luotettuja
Yksityinen / yhteisö	Tai: Organisaatio / Kolmas osapuoli	Organisaatio / Kolmas osapuoli	Organisaation tiloissa / Tilojen ulkopuolella	Luotettuja
Hybridi	Sekä organisaatio että kolmas osapuoli	Sekä organisaatio että kolmas osapuoli	Sekä tiloissa että tilojen ulkopuolella	Sekä luotettuja että ei-luotettuja

Kuva 19: Pilvien sijoitusmallien vertailu [53, s. 22, piirretty uudestaan]

Yhteenvetona pilvien sijoitusmallit tarjoavat organisaatioille erilaisia mahdollisuuksia hyödyntää pilvipalveluja toiminnassaan. Jokaisessa on myös eri piirteitä hallinnoinnin ja omistussuhteiden jakautumisessa, kuten kuva 19 osoittaa. Julkiset pilvipalvelut mahdollistavat palvelun tarjoamisen pienimmillä pääoma- ja hallinnointikustannuksilla, mutta toisaalta niiden tuoma monivuokralaisuus, ei-luotetut käyttäjät ja vähäinen valta infrastruktuurin turvallisuustekijöihin nostavat tietoturvariskejä. Yksityinen pilvipalvelu puolestaan tarjoaa suurimman vallan infrastruktuuriin ja sen tietoturvatekijöihin, eikä sitä koske monivuokralaisuuteen liittyvät tietoturvariskit, mutta se on myös sijoitusmalleista kaikista kallein. Yhteisöpilvi on yksi kompromissi yksityisen ja julkisen pilvipalvelun välillä, missä monivuokralaisuuden tietoturvariskejä lievitetään luottamussuhteella toisiin vuokralaisiin ja heidän käyttäjiinsä, mutta samalla voidaan nauttia kustannuksien jakamisesta yhteisön kesken. Hybridipilvi on varsinaisen kompromissin sijaan yhdistelmä sekä julkisia että yksityisiä pilvipalveluja. Tämä jako mahdollistaa turvallisuuskriittisten palveluelementtien pitämisen yksityisinä ja ei-kriittisten palveluelementtien ajamisen julkisessa pilvessä, mikä säästää kustannuksissa.

6.4 Hyödyt identiteetinhallinnan kannalta

Tämä luku käsittelee pilvipalveluista saatavia hyötyjä identiteetinhallinnan kannalta. Nämä hyödyt jakautuvat kustannuksiin, ylläpitoon sekä resurssien joustavaan käyttöön.

- Pienemmät ja ennustettavammat kustannukset

  Perinteiseen sisäisesti tehtyyn sovelluskehitykseen ja valmiin palvelun ylläpitoon liittyy paljon yleiskustannuksia, kuten esimerkiksi IT-henkilöstön palkkakustannukset, tilakustannukset, laitteistokustannukset sekä laitteiston käytön tuomat sähkö- ja jäähdytyskustannukset. Näitä kaikkia kustannuksia on vaikea arvioida tarkasti suunnitteluvaiheessa ja ne voivat helposti kasvaa korkeammaksi kuin mitä oli suunniteltu. Vaikka pilvipalvelujenkin lopulliset kustannukset riippuvat useista tekijöistä, ne ovat asiakkaan kannalta huomattavasti ennustettavampia, koska sopimuksessa oleva hinta voi usein olla kiinteä kuukausimaksu. Tämä mahdollistaa sisäistä toteutusta halvemman pilvipalveluntarjoajan valitsemisen jo suunnitteluvaiheessa ja poistaa yleiskustannuksiin liittyviä yllätyksiä. [54, s. 6]

- Vähäiset pääomakustannukset

  Pilvipalveluiden vuokramainen maksumalli tekee niihin liittyvistä kustannuksista lähes yksinomaan operaatiokustannuksia asiakkaan taholta. Tämä tarkoittaa, ettei palvelun käytön aloittamiseen tarvita suurta pääomaa, koska mitään erityistä aloitusmaksua ei yleensä ole eikä mitään pääomaa tarvitse hankkia. Lisäksi, verolainsäädännöstä riippuen, pääomakustannuksista eroon pääseminen voi tuoda verohelpotuksia organisaatiolle. [54, s. 6]

- Asiantuntijoiden ylläpitämät järjestelmät

  Pilvipalvelujentarjoajien voidaan yleensä olettaa palkkaavan alansa asiantuntijoita ylläpitämään infrastruktuuriaan sekä sovelluksiaan. Tämä helpottaa asiakasorganisaatioiden toimintaa, koska niiden ei tarvitse itse huolehtia asiantuntevan ylläpitohenkilöstön rekrytoinnista ja kouluttamisesta. [54, s. 6] Lisäksi koska pilvipalveluntarjoajalla on yleensä useita asiakkaita, pilvipalveluntarjoajan palkkaamien asiantuntijoiden hyödyt jakautuvat useille asiakkaille. Tämä tarkoittaa, ettei asiakasorganisaatioiden tarvitse kilpailla keskenään ammattitaitoisista ylläpitohenkilöistä, joita kaikissa työmarkkinatilanteissa ei välttämättä riitä kaikille.

- Tarpeen mukaan skaalautuvat resurssit

  Pilvipalveluissa pystytään lisäämään ja vähentämään resursseja käyttötarpeen mukaan. Tämä voi tapahtua vuokraamalla lisää virtuaalisia palvelimia kiinteillä kuukausimaksuilla tai esimerkiksi laskentatehoa sekunteina. [54, s. 6] Tämä säästää rahaa, koska fyysisiä palvelimia tai muutakaan laitteistoa ei tarvitse ostaa hetkellistä tarvetta varten, jonka jälkeen ne saattaisivat jäädä hyvin vähäiselle käytölle, vaan resursseista maksetaan vain sen mukaan ja sen aikaa kuin niitä oikeasti tarvitaan.

- Nopea resurssien provisiointi

  Kuten edellisessä kohdassa mainittiin, pilvipalvelut mahdollistavat palvelimien tai laskentaresurssien lisäämisen joustavasti tarpeen mukaan. Tämä ei säästä ainoastaan rahaa vaan myös aikaa, koska uusien palvelimien tai sovellusten käyttöönottoon kuluu viikkojen tai kuukausien sijaan minuutteja. [54, s. 7] Tämä voi myös leikata aikaa markkinoille pääsyyn, joka joillain aloilla voi tuoda selkeän kilpailuedun, koska toiminnan voi aloittaa hyvin nopeasti lähes nollatilanteesta.

Useimmat yllä mainituista pilvipalvelujen hyödyistä painottuvat toiminnan aloittamisen ja laajentamisen nopeuteen ja helppouteen sekä kustannustehokkuuteen, mikä ei tule yllätyksenä, sillä ne liittyvät läheisesti luvussa 6.1 avattuihin pilvilaskennan määritelmiin, kuten nopeaan joustavuuteen, suureen skaalautuvuuteen ja käytönmukaiseen maksamismalliin. Tämän pohjalta vaikuttaa siltä, että pilvipalvelut lunastavat pitkälti juuri sen, mitä ne määritelmänsä pohjalta lupaavatkin. Lopullisten hyötyjen suuruus ja keskinäiset mittasuhteet riippuvat kuitenkin aina palveluntarjoajan valinnasta, tehdystä sopimuksesta, palvelumallista sekä sijoitusmallista. Yhteenvetona pilvipalvelujen hyödyt ovat melko yksinkertaisia, mutta vetoavia: palvelut saadaan pystytettyä nopeammin, ylläpidettyä helpommin ja ennustettavammin kustannuksin kuin perinteisillä toteutustavoilla.

6.5 Haasteet

Pilvipalveluihin liittyy perinteisiin teknologioihin verrattuna uusia haasteita ja riskejä. Näitä haasteita ja riskejä esitellään alla ja lopuksi esitellään joitain yleisiä ratkaisuja niihin.

- Maantieteellinen hajauttaminen ja eri lainsäädännöt

  Julkisen pilvipalvelun resurssit ovat hajautettuja, joten asiakas ei voi tietää tarkkaan, missä käytettävät resurssit sijaitsevat ja missä varsinainen tiedon käsittely ja tallennus tapahtuu. Tämä voi aiheuttaa ongelmia, koska esimerkiksi eri maiden sähköistä tiedonkäsittelyä ja henkilötietojen käsittelyä koskevat lainsäädännöt ovat erilaisia. Pilvipalveluntarjoajat voivat esimerkiksi joutua luovuttamaan asiakkaan tietoja jonkin vieraan maan viranomaisille perusteilla, joiden pohjalta tietojen luovuttaminen asiakkaan kotimaassa olisi lainvastaista. [55, s. 3] Lisäksi lainsäädäntö voi estää esimerkiksi henkilötietojen käsittelyn – varsin olennaisen asian identiteetinhallintajärjestelmien kannalta – pilvipalvelussa, jos tiedot ylittävät valtion rajat. Esimerkiksi EU:n direktiivin 95/46/EY [56, artikla 25] kieltää henkilötietojen siirtämisen EU:n ulkopuolisiin maihin, joissa tiedolla ei katsota olevan riittävän korkeaa suojaa. Poikkeuksena kieltoon mainitaan lähinnä henkilön *yksiselitteinen* suostumus tietojen siirtoon tai että siirron on oltava muilla [56, artikla 26] tavoin henkilön tai yleisen edun mukaista. Tällaiset lakitekniset yksityiskohdat voivat tehdä sekä palveluntarjoajan että asiakkaan toiminnasta hyvin hankalaa.

- Monivuokralaisuus [57, s. 249]

  Monivuokralaisuuden pohjimmainen riski tulee siitä, että samalla fyysisellä laitteistolla käsitellään eri asiakkaiden tietoja samanaikaisesti. Tämä mahdol-

listaa tietojen vuotamisen vahingossa tai tarkoituksellisten hyökkäyksien kautta toisille vuokralaisille. [55, s. 4] Pilvipalveluntarjoajan on varmistuttava, että jokaisen asiakkaan tiedot pysyvät eroteltuina koko elinkaarensa ajan ja asiakkaan on käytännössä luotettava tähän lupaukseen.

- Luottamuksellisuus

  Tietojen tallentaminen ja käsittely pilvipalvelussa edellyttää yleensä, että kaikki tiedot ovat saatavilla Internetin kautta, mikä helpottaa mahdollisia hyökkäyksiä, koska asiakkaan fyysisiä turvajärjestelyjä ei tarvitse ohittaa lainkaan. [58, s. 15–16] Perinteisesti sellaisia tietoja, joiden luottamuksellisuus on hyvin tärkeää, on voitu säilyttää ja käsitellä järjestelmissä, jotka on täysin erotettu julkisista verkoista ja mahdollisesti vielä suojattu fyysisillä turvatoimilla, kuten lukituilla tiloilla, kulunvalvonnalla ja vartioinnilla [59, s. 399–401]. Tällainen ei kuitenkaan ole yleensä mahdollista pilvipalvelussa, koska jos sovelluksia ajetaan pilvipalvelussa, joka sijaitsee julkisessa verkossa, kaikki niiden käsittelemä tieto on silloin myös julkisessa verkossa riippumatta sen tärkeydestä.

- Lukittautuminen

  Pilvipalvelujen toteutuksessa käytetään usein patentoituja tai ei-standardoituja ohjelmointirajapintoja, mikä hankaloittaa tai jopa estää asiakkaita siirtämästä tietojaan esimerkiksi toiseen pilvipalveluun. Tämä käytännössä lukitsee pilvipalvelun asiakkaan yhteen palveluntarjoajaan, mikä tuo mukanaan riskit hinnoittelun noususta, luotettavuuden laskusta ja palveluntarjoajan mahdollisen konkurssin hyvin rampauttavasta vaikutuksesta asiakkaan toimintaan. Pilvipalveluntarjoajan näkökulmasta tilanne on päinvastainen ja jopa houkutteleva, koska lukittautuminen sitoo maksavat asiakkaat heidän palveluunsa. [58, s. 15]

- Tiedonsiirron pullonkaulat

  Modernit sovellukset käyttävät yhä kasvavia määriä tietoa ja julkisissa pilvipalveluissa tämä tieto siirretään Internetin yli. Tämän kasvavan tietomäärän siirron myötä tulevat kasvavat kustannukset kuten myös kasvavat siirtoajat. Asiakkaat ja pilvipalvelun tarjoajat joutuvat miettimään tarkkaan tarvitsemiaan tiedonsiirtomääriä ja niiden sijoittamista järjestelmän eri tasoille. Internetin ohella tiedonsiirron rajoitukset voivat tulla vastaan myös pilvipalvelun sisäisessä verkkoinfrastruktuurissa, missä yksittäisten etenkin alemmilla tasoilla olevien verkkoelementtien kaistanleveys voi muodostua rajoittavaksi tekijäksi. [58, s. 16]

- Suorituskyvyn ennustamattomuus

  Pilvilaskennassa jaetut prosessointi- ja muistiresurssit toimivat hyvin ja niiden suorituskyky on ennustettavaa, mutta levyresurssien tapauksessa tilanne on huonompi. Samalla järjestelmällä, jossa ajettiin 75 rinnakkaista instanssia, muistin suorituskyvyn keskipoikkeama oli alle 4 prosenttia keskiarvosta kun taas levyoperaatioiden tapauksessa keskipoikkeama keskiarvosta oli yli 16 prosenttia. [58, s. 17] Asiakkaalla ei myöskään ole yleensä näkyvyyttä resurssien todelliseen määrään, koska pilvipalvelun yksi perusominaisuuksista on

abstrahoida nämä resurssit näennäisesti loputtomaksi pooliksi. Kuitenkin todellisuudessa resurssit ovat rajalliset ja ne voivat loppua kesken, jos asiakastarpeita tai niiden kasvua ei ole otettu oikein huomioon resurssien mitoituksessa pilvipalveluntarjoajan osalta. Mikäli pilvipalvelun kapasiteetti on mitoitettu väärin ja resursseja yritetään käyttää yli rajojen, tämä saattaa kaataa joko yksittäisiä pilvi-infrastruktuurin palvelimia tai pahemmassa tapauksessa koko pilvi-infrastruktuurin [57, s. 249].

- Tallennetun tiedon integriteetti

  Integriteetissä on kyse tiedon oikeellisuudesta ja muuttumattomuudesta. Mikäli asiakkaan pilvipalveluun tallennetut kriittiset tiedot muuttuvat tai tuhoutuvat, ei asiakkaalla itsellään ole välttämättä mitään keinoja vaikuttaa tietojen palauttamiseen, koska viime kädessä kaikki tiedot ja prosessit ovat palveluntarjoajan hallitsemassa laitteistossa. Mutta vastuu tiedon muuttumattomuudesta ei ole välttämättä yksiselitteisesti palveluntarjoajalla. [57, s. 250] Jos asiakas esimerkiksi tallentaa omien asiakkaidensa tietoja pilvipalveluun ja ne tuhoutuvat tai muuttuvat haitallisesti, onko lakitekninen vastuu ja korvausvastuu pilvipalveluntarjoajan, asiakkaan vai kenties asiakkaan asiakkaan harteilla.

- Saatavuus

  Mahdollisuus lähes keskeytymättömälle saatavuudelle on ollut yksi suurimmista eduista, joilla pilvipalveluja on markkinoitu [57, s. 249–250]. Kuitenkin vuonna 2008 Berkeleyn yliopiston tekemässä tutkimuksessa suuretkin pilvipalveluntarjoajat, joiden infrastruktuurit olivat markkinoiden parhaita, kuten Amazon (S3) ja Google (AppEngine ja Gmail), kärsivät tuntien katkoksista neljän kuukauden tutkimusjakson aikana. Katkokset johtuivat muun muassa ohjelmointivirheistä, yhden bitin virheestä viestintäprotokollassa ja pääsynhallintajärjestelmän ylikuormituksesta. Yhteinen heikkous katkoksien taustalla oli se, että vaikka pilvipalvelujen yleensä ajatellaan kiertävän yhden heikon pisteen (engl. single point of failure) ongelman hajautetulla infrastruktuurillaan, niillä onkin itse asiassa usein tällainen piste – pilvipalvelua tarjoava yritys. Vaikka pilvipalvelun resurssit olisivatkin maantieteellisesti hajautettu, ne saattavat silti jakaa saman sovellusinfrastruktuurin tai hallintoa. Pahimmassa tapauksessa yksittäinen palvelua tarjoava yritys voi mennä konkurssiin, mikä lopettaisi koko palvelun. [58, s. 14]

- Järjestelmän valvonta- ja lokitiedot

  Yhä useampien tärkeiden sovellusten siirtyessä pilvipalveluihin, asiakkaat tulevat haluamaan entistä enemmän valvonta- ja lokitietoja järjestelmästä. Kuitenkin nämä tiedot sisältävät usein sensitiivistä tietoa palveluntarjoajien infrastruktuureista, eivätkä palveluntarjoajat yleensä ole halukkaita jakamaan tätä tietoa muille. Tilanne on ongelmallinen molempien osapuolien kannalta ja edellyttää yleensä paljon neuvottelua ennen kuin jonkinlaiseen kompromissiin tai sopimukseen päästään. [55, s. 4]

Osaa yllä mainituista riskeistä voidaan hallita asiakkaan taholta sopivilla palveluehtosopimuksilla (engl. service license agreement, SLA), jotka määrittelevät ehtoja ja vastuita, jotka pilvipalveluntarjoajan on täytettävä. [57, s. 249–250] Hajautettuihin

resursseihin liittyviä lakiongelmia voidaan pyrkiä vähentämään esimerkiksi valitsemalla pilvipalveluntarjoaja, jonka koko infrastruktuuri on sijoitettu yhden valtion rajojen sisälle tai varmistamalla sopimustasolla, että vaikka infrastruktuuri jakautuisikin useisiin maihin, tietoja käsiteltäisiin vain sillä osalla infrastruktuuria, joka sijaitsee lainsäädännön kannalta sopivissa maissa.

Monivuokralaisuuteen ja luottamuksellisuuteen liittyviä riskejä voidaan osittain lieventää sisällyttämällä pääsynhallinnan ulkoinen auditointi sopimuksen ehtoihin [57, s. 249], jotta tietoturvan tasosta voidaan olla varmempia. Monivuokralaisuuden riskejä on kuitenkin hyvin hankala hallita julkisissa pilvipalveluissa, joten varmin tapa vähentää sen tuomia riskejä on sijoittaa kriittiset toiminnot yksityiseen pilveen tai organisaation omaan infrastruktuuriin. Tietojen integriteettiin, suorituskyvyn ennustamattomuuteen ja palvelun saatavuuteen puolestaan voidaan vaikuttaa suoraan asettamalla palveluehtosopimuksessa määreet sille, kuinka suuren osan ajasta palvelun on oltava saatavilla, millä resursseilla ja millä todennäköisyydellä tiedot pysyvät eheinä [57, s. 250].

Lukittautumiseen voidaan vaikuttaa esimerkiksi valitsemalla sellaisia palveluntarjoajia, jotka käyttävät avoimia standardeja ja joista tiedot voidaan siirtää mahdollisimman vaivattomasti toiseen järjestelmään. Samaan tapaan valvonta- ja lokitietoihin pääsy voi olla palveluntarjoajan valinnasta kiinni, vaikka siihen voidaan aina myös yrittää vaikuttaa sopimusehdoilla. Tiedonsiirron pullonkauloja voidaan kiertää osittain palvelunehtosopimuksilla, mutta mikäli tarvittavaa kaistanleveyttä ei vain ole tarjolla, voidaan harkita myös tiedon siirtoa perinteisillä postipalveluilla [58, s. 18]. Esimerkiksi postittamalla kymmenen teratavua yhden teratavun kovalevyinä hieman yli 1000 kilometrin päähän voidaan leikata tiedonsiirtokustannukset puoleen ja tiedonsiirtoviive jopa 45-osaan verrattuna tiedonsiirtoon internetin 20 Mbps nopeudella [58, s. 18]. Tällainen fyysinen tiedonsiirtotapa ei kuitenkaan sovellu kaikkiin tarkoituksiin.

Yhteenvetona pilvipalveluihin liittyy paljon sekä uusia että hieman tutumpia haasteita ja riskejä. Moniin näistä voidaan vaikuttaa ainakin jossain määrin palvelunehtosopimuksilla tai valitsemalla sopiva palveluntarjoaja. Lisäksi voidaan yrittää käyttää mielikuvitusta haasteiden suhteen ja yrittää lähestyä niitä aivan eri näkökulmasta, kuten tiedonsiirron pullonkaulojen ohittaminen fyysisellä postituksella. Kuitenkin on huomioitava, että tässä luvussa esiteltiin vain tunnettuja haasteita ja riskejä. Näin uuteen ja nopeasti kehittyvään teknologiaan voi liittyä lukuisia toistaiseksi tuntemattomia riskitekijöitä, jotka voivat heikentää sopimuksiin perustuvaa turvallisuutta, koska sopimuksia tehtäessä ei ole ollut vielä täyttä ymmärrystä kaikista palveluun vaikuttavista riskitekijöistä. Tämän pohjalta pilvipalveluihin siirtymisessä on syytä erityiseen tarkkaavaisuuteen ja harkintaan riskitekijöiden osalta.

6.6 Identiteetinhallinta pilvipalveluna

Identiteetinhallinta palveluna (engl. Identity as a Service, IDaaS) tarkoittaa pohjimmiltaan pilvipalveluna toteutettua palvelua, jossa kolmas osapuoli suorittaa identiteetinhallintatehtäviä, kuten identiteettien elämäkaarenhallintaa, tai pääsynhallintaa. Tämä termi kattaa periaatteessa kaikki toteutukset millä tahansa pilvipalvelu- tai sijoitusmallilla aina palveluna tarjottavasta ohjelmistosta palveluna tarjottavaan infrastruktuuriin, yksityisestä pilvestä julkiseen tai hybridipilveen. [60, s. 33]

Identiteetinhallinta pilvipalveluna on vielä tuore suuntaus pilvipalvelujen piirissä eikä se ole vielä ehtinyt kovin kypsälle tasolle. Lisäksi eri palvelumallit ovat vielä keskenään eri kehitysvaiheissa, kuten Mather et al. tekemä arvio taulukossa 6.1 näyttää. Taulukossa on kuvattu kunkin palvelumallin kyvykkyystaso epäkypsä–tiedostava–kyvykäs -asteikolla ja lisäksi tiivistetty lyhyesti kunkin kypsyystason kriteerit arvioiduilla identiteetinhallinnan osa-alueilla. Alkuperäinen asteikko jatkuu vielä kypsään ja lopulta johtavaan, mutta yksikään palvelumalleista ei saavuttanut näitä kypsyysasteita. Taulukon perusteella palveluna tarjottava ohjelmisto on pisimmälle kehittynyt pohja identiteetinhallinnalle pilvipalveluna, koska sen kypsyystasot ovat korkeimmalla tasolla arvioiduista palvelumalleista jokaisella osa-alueella. Palveluna tarjottava infrastruktuuri tulee toisena, tarjoten kyvykkään todennuksenhallinnan ja tiedostavan käyttäjähallinnan uusien identiteettien luomisen kannalta, vaikka sen identiteettien muutosten toteutus ja valtuutuksenhallinta ovatkin epäkypsällä tasolla. Palveluna tarjottava palvelualusta saa ryhmän huonoimmat arviot jokaisessa kategoriassa. Se arvioitiin epäkypsäksi kaikissa paitsi todennuksenhallinnassa, jossa se arvioitiin pelkästään tiedostavaksi.

Taulukko 6.1. Pilvipalvelumallien kypsyysasteet identiteetinhallinnan kannalta [51, yhdistetty taulukoista 5.2 ja 5.3]

Osa-alue	**SaaS**	**PaaS**	**IaaS**
Käyttäjähallinta, uusien käyttäjäidentiteettien luominen	**Kyvykäs**: ▪Automatisoitu soveltuvilta osin ▪Erotellut prosessit	**Epäkypsä:** ▪Manuaalinen, tarpeen mukaan toteuttava, ilman formaalia prosessia	**Tiedostava:** ▪Manuaalinen, tarpeen mukaan toteutettava, noudattaen muodostettuja prosesseja
Käyttäjähallinta, käyttäjäidentiteettien muutokset	**Kyvykäs**: ▪Manuaalinen tai automatisoitu sovellusryhmäkohtaisesti	**Epäkypsä:** ▪Manuaalinen, tarpeen mukaan toteutettava, sovelluskohtainen	**Epäkypsä:** ▪Manuaalinen, tarpeen mukaan toteutettava, sovelluskohtainen
Todennuksenhallinta	**Kyvykäs**: ▪Yleinen todennusmekanismi ▪Ei yleistä todennusmoduulia	**Tiedostava:** ▪Käsitellään sovelluskohtaisesti Ei yleistä todennusmekanismia	**Kyvykäs**: ▪Yleinen todennusmekanismi ▪Ei yleistä todennusmoduulia
Valtuutuksenhallinta	**Tiedostava:** ▪Käsitellään sovelluskohtaisesti ▪Ei yleistä valtuutusmekanismia	**Epäkypsä:** ▪Manuaalinen, tarpeen mukaan toteutettava, ei sääntö- tai roolipohjaista valtuutusta	**Epäkypsä:** ▪Manuaalinen, tarpeen mukaan toteutettava, ei sääntö- tai roolipohjaista valtuutusta

Tutkimuksessa saatujen tulosten pohjalta palveluna tarjottava ohjelmisto vaikuttaa pilvipalvelumallien monipuolisimmalta ja kyvykkäimmältä palvelumalliehdokkaalta tämänhetkisille identiteetinhallinta palveluna -toteutuksille. Se hyötyy kaikista luvussa 6.4 mainituista palveluna tarjottavan ohjelmiston eduista, kuten alennetuista aloituskustannuksista sekä pilvipalveluntarjoajan kantamasta palvelun ylläpitovastuusta. Toisaalta palveluna tarjottava ohjelmisto kantaa myös yleiset luvussa 6.5 käsitellyt julkista pilvipalvelua koskevat riskit. Esimerkiksi asiakkaan omien työntekijöiden identiteettien käsittely ja tallennus tapahtuu julkisessa verkossa olevassa infrastruktuurissa, jolloin identiteetit ovat alttiimpia uhkille, mikä voi edelleen johtaa asiakkaan

sisäisten järjestelmien vaarantumiseen [60, s. 34]. Tämä tarkoittaa, että asiakkaan pitää selvittää tarkkaan, miten esimerkiksi pilvipalveluntarjoajan todennus tapahtuu, miten hyvin tallennettuja ja siirrettäviä tietoja suojataan sekä kaikki muut asiakkaan oman tietoturvapolitiikan kannalta tärkeät asiat [60, s. 34].

Palvena tarjottava palvelualusta tarjoaa vähiten monipuolisuutta ja kyvykkyyttä identiteetinhallinnan suhteen kaikista palvelumalleista. Sitä koskee käytännössä samat identiteetinhallintahaasteet, jotka koskevat palveluna tarjottavaa ohjelmistoa, ja sen lisäksi mahdolliset haasteet asiakkaan oman sovelluksen ja palvelualustan välisessä vuorovaikutuksessa. Asiakkaan pitää itse selvittää ja suunnitella, miten identiteetit provisioidaan ja deprovisioidaan, minne identiteettitiedot tallennetaan ja miten niihin päästään käsiksi. Lisäksi asiakas joutuu järjestelmään palveluntarjoajan kanssa, miten todennus ja mahdolliset jäljitysketjujen kirjaukset hoidetaan. [60, s. 35]

Palveluna tarjottava infrastruktuuri soveltuu kyvyiltään pääasiassa infrastruktuurin päällä ajettavien virtuaalikoneiden pääsynhallintaan. Tätä palvelumallia käyttävät identiteettipilvipalveluntarjoajat tarjoavatkin yleensä pääsynhallintaa, kuten esimerkiksi kertakirjautumista, palveluna tarjottaville palvelualustoille sekä ohjelmistoille. [60, s. 35]

Pilvipalvelun eri sijoitusmallit tarjoavat myös eri vaihtoehtoja identiteetinhallinnan toteuttamiselle pilvipalveluna. Sen sijaan, että koko identiteetinhallintapalvelu olisi julkisessa pilvipalvelussa, voidaan käyttää hybridiratkaisuja, joissa osa identiteetinhallintakomponenteista on julkisessa pilvessä ja esimerkiksi käyttäjätietojen varasto oman organisaation kiinteistön sisällä palomuurin takana. Tämä ratkaisee ainakin identiteettien julkiseen pilveen varastoimisesta aiheutuvat huolet, mutta toisaalta kasvattaa ylläpitovastuuta sekä aloittamisen pääomakustannuksia, ellei organisaatiolla ole olemassa olevaa infrastruktuuria käyttäjähakemistoille. [51, s. 94–96]

6.7 Yhteenveto

Pilvilaskenta tarkoittaa laskennan, tiedon tallentamisen ja hallinnoimisen hoitamista ryhmällä etäpalvelimia paikallisten palvelimien sijaan. Sen keskeisiä ominaispiirteitä ovat muun muassa monivuokralaisuus eli useiden eri asiakkaiden palvelujen ajaminen samalla infrastruktuurilla, kymmenien tuhansien järjestelmien kertaluokkaan yltävä skaalautuvuus sekä joustavasti ja nopeasti laskentatarpeisiin mukautuvat resurssit. Nämä ominaispiirteet toteutetaan virtualisoinnilla, joka mahdollistaa kaikkien infrastruktuuriresurssien jakamisen loogisiin eli virtuaalisiin, kokonaisuuksiin kuten erillisiksi palvelimiksi, prosessoreiksi tai tallennuslevyiksi.

Pilvilaskennalla toteutettuja palvelukokonaisuuksia kutsutaan pilvipalveluiksi tai pilviksi. Pilvipalveluntarjoaja vuokraa pilvipalveluinfrastruktuuria asiakkaille, jotka voivat käyttää tätä infrastruktuuria ajaakseen sovelluksia joko omaan käyttöönsä tai eteenpäin myytäviksi palveluiksi. Pilvien palvelumallit kuvaavat sitä, mitä teknologiakerroksia asiakas voi pilvipalveluntarjoajalta vuokrata. Yleisimmät näistä ovat palveluna tarjottava yksittäinen sovellus (SaaS), palveluna tarjottu palvelualusta (PaaS), jolla voidaan kehittää ja ajaa useita sovelluksia, sekä palveluna tarjottu infrastruktuuri (IaaS). Pilvien sijoitusmallit puolestaan kuvaavat sitä, miten pilvien omistajuus, hallinnointivastuut ja fyysinen sijainti määräytyvät. Nämä sijoitusmallit jakautuvat julkiseen pilveen, jossa kolmas osapuoli omistaa ja hallinnoi koko pilveä, yksityiseen tai yhteisöpilveen, joissa omistajuus ja hallinnointivastuut voivat olla täysin yksityisiä tai

yhteisön sisäisiä tai sitten jakautua osittain yksityisten osapuolten ja kolmannen osapuolen välillä, sekä hybridipilveen, jossa osa pilvestä on julkista pilveä ja osa yksityistä.

Identiteetinhallinnan kannalta pilvipalveluissa on sekä hyötyjä että haasteita. Hyödyt keskittyvät pienempiin ja ennustettavampiin kustannuksiin, tarpeenmukaiseen skaalautuvuuteen ja nopeaan resurssien joustavuuteen, mitkä mahdollistavat aiempaa halvemman ja nopeamman toiminnan aloittamisen sekä kasvattamisen. Nämä hyödyt korostuvat etenkin palveluna tarjotussa identiteetinhallinnassa (IDaaS), jossa säästöt kohdistuvat nimenomaan identiteetinhallintajärjestelmään kokonaisuuden sijaan. Valitettavasti pilvipalveluihin liittyy myös haasteita ja riskejä identiteetinhallinnan kannalta. Monivuokralaisuus ja ylipäätään verkkoon sijoitettu palvelu aiheuttavat uhkia niissä käsiteltävien tietojen luottamuksellisuudelle ja integriteetille, koska luottamuksellisuutta tai integriteettiä ei voida itse paikallisesti valvoa. Suorituskyvyn ja saatavuuden ennustamattomuus pilvipalveluissa voivat taas aiheuttaa yllättäviä ja suuria takaiskuja toiminnalle, eikä niihinkään voida juuri paikallisesti vaikuttaa. Viimeisenä muttei vähäisimpänä maantieteellinen hajautus ja tietojen- sekä henkilötietojen käsittelyä koskevat säädökset ja lait muodostavat juridisia riskejä, koska tietoa saatetaan käsitellä maissa, jonne sitä ei saisi lain, sopimuksien tai säädöksien mukaan edes siirtää. Useimpia näistä haasteista voidaan hallita jossain määrin palvelunehtosopimuksilla, mutta lopullista turvaa niillä ei voida saavuttaa.

Pilvipalvelut ovat vielä uutta teknologiaa, johon liittyy runsaasti epävarmuuksia ja haasteita, mutta toisaalta myös houkuttelevia lupauksia tehokkuudesta ja säästöistä. Etenkin palveluna tarjottava identiteetinhallinta on vielä tässä vaiheessa varsin epäkypsässä kehitysvaiheessa, mutta toisaalta se on varmasti houkutteleva vaihtoehto etenkin pienemmille organisaatioille. Perinteisemmässä tapauksessa pilvipalvelujen vaikutus identiteetinhallintaan on lopulta hyvin tapauskohtaista riippuen hallinnoitavien järjestelmien sijoitus- ja palvelumalleista, niiden kokonaisosuudesta järjestelmissä sekä käyttötarpeesta. Täysin julkiset pilvet ovat ongelmallisia, koska henkilötietoja joudutaan käytännössä väistämättä käsittelemään julkisessa verkossa lukuisten vuokralaisten kanssa jaetulla infrastruktuurilla. Yksityiset pilvet puolestaan antavat perinteisen tyyppistä ja tuttua turvaa henkilötiedoille, mutta menettävät samalla suuren osa pilvipalvelun kustannussäätöistä. Yhteisöpilvet tarjoavat kompromissin yksityisten ja julkisten väliltä yksityistä pilveä jonkin verran matalammin kustannuksin, mutta julkista pilveä paremmalla turvallisuudella. Hybridipilvissä kriittiset osat voidaan sijoittaa yksityiseen ja loput julkiseen pilveen, mikä mahdollistaa turvallisuuden ja kustannuksien keskinäisen suhteen optimoinnin. Tällä tavoin sijoitetut hybridipilvet vaikuttavatkin tällä hetkellä yleisesti helpoimmalta tavalta saada identiteetinhallinta ja pilvipalvelut toimimaan yhdessä melko turvallisesti, mutta uhraamatta toisaalta liiaksi pilvipalvelujen tuomia hyötyjä. Lähestymistapa nojaa turvallisuuden suhteen perinteiseen malliin, jossa organisaatiot kontrolloivat itse kriittisiä tietoja, koska niitä ei uskota muiden haltuun tai julkiseen verkkoon. Lopulta muun kehityksen mennessä kohti pilvipalveluja tulee pilviteknologia väistämättä vaikuttamaan merkittävästi myös identiteetinhallintaan sekä sen teknologian ja periaatteiden kehitykseen. Tämän kehityksen myötä vanhojen turvallisuusmallien rinnalle tulee nousemaan uusia pilvikeskeisempiä turvallisuusmalleja, jotka mahdollistavat uudenlaisia tapoja toteuttaa identiteetinhallinnan ja pilvipalvelujen yhteiselo turvallisesti.

7 Yhteenveto

Tämän diplomityön tarkoitus oli luoda katsaus nykyisiin identiteetinhallintateknologiaan, sillä toteutettuihin tuotteisiin sekä teknologian tulevaisuuden näkymiin. Työn teoriaosuuden toisessa ja kolmannessa luvuissa on selitetty identiteetinhallinnan ja digitaalisen identiteetin peruskäsitteet ja keskeisimmät toiminnot sekä kuvattu identiteetin- ja pääsynhallinnan keskeisimpiä protokollia ja standardeja. Teoriaosuus jatkuu vielä neljännen luvun alussa, jossa aiempien lukujen käsitteet ja teknologiat on vedetty yhteen geneerisen arkkitehtuurikuvauksen muodossa.

Loppuosassa neljättä lukua siirryttiin teoriaosuutta konkreettisempaan suuntaan esittelemällä ja vertailemalla keskenään nykyisiä identiteetinhallintatuotteita perustuen Forrester Inc. -tutkimusyhtiön tekemään tutkimukseen vuodelta 2009. Vertailussa tuotteita arvioitiin identiteetin- ja pääsynhallinnan keskeisimpien teknologisten kyvykkyyksien sekä loppukäyttäjien antamien arvioiden pohjalta. Vertailun tulosten perusteella selvisi, että tuotekenttä identiteetinhallinnassa on ominaisuuksiltaan hyvin monimuotoista ja suurimmalla osalla tuotteista oli hyvin selkeitä heikkouksia ja vahvuuksia. Tämä tarkoitti sitä, että tulosten pohjalta tuotteita ei voitu asettaa varsinaiseen paremmuusjärjestykseen, vaan jokaisen tuotehankintaa harkitsevan organisaation on mietittävä hyvin tarkkaan omat tarpeensa ja valittava niihin kaikkein sopivin tuote. Muutama tuote tarjosi selkeästi keskimääräistä tasaisemman ja korkeamman kyvykkyyden, mikä näkyi korkeana keskiarvona eri ominaisuuksien pisteytyksistä. Tämän keskiarvon perusteella kolme vertailussa parhaiten menestynyttä tuotetta olivat Oracle arvosanalla 4,08, CA arvosanalla 3,49 ja Sun Microsystems arvosanalla 3,42 asteikolla nollasta viiteen.

Viidennessä luvussa kartoitettiin asiantuntijoiden näkemystä identiteetinhallintateknologian ja tuotteiden nykytilasta, niiden vahvuuksista ja heikkouksista sekä merkittävistä tulevaisuuden trendeistä. Kartoitus toteutettiin Internetissä lomakepohjaisena kyselytutkimuksena, joka sisälsi sekä kvantitatiivisia että avoimia kysymyksiä. Kyselyyn vastasi kaikkiaan 22 identiteetin- ja pääsynhallintajärjestelmien asiantuntijaa eri puolilta maailmaa. Työkokemuksensa vuosina ilmoittaneiden 17 vastaajan keskimääräinen työkokemus oli 8,3 vuotta, mikä tuki hyvin oletusta keskimääräisestä asiantuntijuudesta. Vastaajamäärä jäi valitettavasti toivottua vähäisemmäksi ja tämän vuoksi vain osa kvantitatiivisista vastauksista oli tilastollisesti merkittäviä halutulla 95%:n luottamusvälillä.

Tilastollisesti merkittäviä kvantitatiivisia tuloksia asteikolla yhdestä viiteen oli muun muassa, että identiteetinhallintajärjestelmien käyttöönottoa ja konfigurointia pidettiin selkeästi vaikeana (3,95 ± 0,36), mikä kielii selkeästä parannuksen tarpeesta asian suhteen. Muita parannusta kaipaavia toiminnallisuuksia olivat raportointi (3,86 ± 0,40), monitorointi (3,76 ± 0,48), käytettävyys loppukäyttäjille (4,00 ± 0,39), delegointi ja itsepalvelu (3,76 ± 0,45) sekä roolienhallinta (3,57 ± 0,45). Ainoastaan yhden ominaisuuden kohdalla tilastollisesti merkittävä tulos tuki sitä, että parannusta ei juurikaan kaivattu, nimittäin hakemistopalveluissa (2,05 ± 0,38). Kvantitatiivisia tuloksia kerättiin myös tulevaisuuden trendien merkityksestä. Kaikkia kysymyksissä listattuja trendejä eli pilvipalveluja (4,05 ± 0,39), mobiileja päätelaitteita teknisestä näkökulmasta (4,05 ± 0,37), käyttäjäkeskeistä identiteetinhallintaa (3,67 ± 0,45), Bring Your Own Device- käytäntöjä (3,73 ± 0,46) ja kontekstisidonnaista identiteetin-

hallintaa (3,90 ± 0,33), pidettiin vastaajien mielestä merkittävinä. Kaikki trendien tuloksista olivat myös tilastollisesti merkittäviä. Näitä tuloksia voidaan käyttää muun muassa ohjaamaan teknologia- ja tuotekehitystä, jotta voitaisiin keskittyä ongelma-alueiden korjaamisen jo riittävinä pidettyjen ominaisuuksien sijaan.

Kyselyn avoimissa kysymyksissä kysyttiin osittain samoja aihepiirejä kuin kvantitatiivisissa kysymyksissä. Tämä tehtiin osittain siksi, että jotain tuloksia saataisiin vaikka vastaajamäärä jäisi liian pieneksi kvantitatiiviselle analyysille ja osittain siksi, että ohjailemattomammat kysymykset voivat tuoda kokonaan uusia mielenkiintoisia näkemyksiä esiin. Vastauksista poimittiin useimmiten eri vastauksissa toistuneita näkemyksiä, jotta näkemyksiä voitaisiin verrata toisiinsa merkityksellisyyden kannalta, koska avoimuuden vuoksi vastaukset olivat enimmäkseen melko hajanaisia. Identiteetin- ja pääsynhallintajärjestelmien vahvuuksina listattiin useimmiten elinkaarenhallinta (6), pääsynhallinta (6), provisiointi (5) ja todentaminen (4). Heikkouksien yleisimmin mainitut olivat huono integroituvuus ja monimutkaisuus. Suurimpina uhkina identiteetinhallinnan teknologialle pidettiin toteuttamisen liian pitkää kestoa (5) ja sen korkea hintaa (4). Kvantitatiivisissa kysymyksissä mainittujen trendien kehityksen suurimpina uhkina tai esteinä pidettiin muutosvastarintaa (3) ja yksityisyyshuolia (3). Avoimien kysymysten vastauksissa tuli myös esiin uusi trendi eli uusien lakien ja säädöksien vaikutukset.

Kuudennessa luvussa paneuduttiin syvemmin yhteen merkityksellisimmäksi pidetyistä identiteetinhallintajärjestelmiin vaikuttavaan trendiin eli pilvipalveluihin. Luvun alussa avattiin pilvilaskennan peruskäsitteet ja -toiminnallisuudet sekä esiteltiin pilvipalvelujen palvelu- ja sijoitusmalleja. Loppuosassa käsiteltiin pilvipalveluiden etuja ja riskejä, jotka vaikuttavat identiteetinhallintaan, sekä itse identiteetinhallintapalvelun toteuttamista pilvipalveluna. Luvussa selvisi, että pilvipalvelut tuovat pääasiassa rahallisia hyötyjä kuten nopeamman ja halvemman verkkopalvelun käytön aloittamisen ja resurssien dynaamisen kasvattamisen tarpeen mukaan sekä kokonaisuudessaan paremmin ennustettavat kustannukset. Toisaalta selvisi myös, että näin tuoreeseen teknologiaan liittyy vielä runsaasti tunnettuja ja tuntemattomia riskitekijöitä, joita pystytään pääasiassa hallitsemaan lähinnä palveluehtosopimuksilla, joskin osittain myös suunnitteluratkaisuilla. Lisäksi monet pilvipalvelujen taloudelliset hyödyt realisoituvat lähinnä julkisessa pilvipalvelussa, joka taas on kaikista korkeariskisin vaihtoehto identiteetinhallinnan kannalta. Identiteetinhallintajärjestelmän pilvipalveluna toteuttamisen kannalta teknologian kypsyys vaihtelee paljon palvelumallin mukaan. Palveluna tarjottavana ohjelmisto on näistä pisimmälle kehittynein ja se on kyvykäs uusien käyttäjien luomisessa, muutoksissa ja todennuksen hallittavuudessa. Valtuuttamisen osalta hallinta jää kuitenkin tiedostavalle asteelle. Palveluna tarjottava infrastruktuuri kykenee todennuksenhallintaan ja siinä on myös tiedostavan tasoinen uusien käyttäjien luominen, mutta muilta osin se jää epäkypsälle tasolle. Kaikista epäkypsin kolmesta palvelumallista on palveluna tarjottava palvelualusta, jossa on vain tiedostavan tasoinen todennuksenhallinta kaikkien muiden toiminnallisuuksien ollessa vielä epäkypsiä. Johtopäätöksenä pilvipalvelut tuovat vielä tällä hetkellä enemmän riskejä kuin hyötyjä identiteetinhallinnan kannalta, mutta toisaalta pilviteknologia on nyt niin vahvasti esillä, että sen voi kehittyä hyvin nopeastikin. Siispä vaikka pilvipalveluihin tuleekin vielä suhtautua etenkin identiteetinhallinnan kannalta varauksella, tarkkaan harkitut ja toteutetut pioneerikokeilut voivat luoda arvokasta lisätietoa aiheeseen ja ajaa kehitystä nopeammin parempaan suuntaan. Palveluna tarjottavana ohjelmistona toteutettu identiteetinhallintajärjestelmä voisi esimerkiksi toimia kokeilunarvoisena

ratkaisuna, jos tarvitaan vain hyvin yksinkertainen identiteetinhallintajärjestelmä matalin kustannuksin ja ennen kaikkea nopeasti.

8 Lähdeluettelo

[1] Identiteetti. [Online]. SuomiSanakirja.fi. [Viitattu 4.8.2012]. Saatavissa: http://suomisanakirja.fi/identiteetti.

[2] Bertino, E., Takahashi, K. Identity Management: Concepts, Technologies, and Systems. Artech House, Incorporated, 2011. 196 s. ISBN 9781608070398 (painettu).

[3] Windley, P. Digital Identity. O'Reilly Media, 2005. 277 s. ISBN 9780596008789 (painettu).

[4] ITU-T Y.2720. NGN identity management framework. International Telecommunication Union, 2009. 34 s.

[5] Oostdijk, M. et al. Provisioning scenarios in identity federations. GigaPort3. Surfnet, 2010. [Viitattu 28.06.2012]. Saatavissa: http://www.surfnet.nl/nl/Innovatieprogramma's/gigaport3/Documents/EDS-4%20Provisioning%20Scenarios%20in%20Federations%20Final.pdf.

[6] Bresz, F., Rai, S., Institute of Internal Auditors. Global Technology Audit Guide 9: Identity and Access Management. Inst of Internal Auditors, 2007. ISBN 9780894136177 (painettu).

[7] von Solms, B., von Solms, R. The 10 deadly sins of information security management. Computers & Security. [Verkkolehti] Vol. 23:5, 2004. S. 371–376. [Viitattu 8.9.2012]. DOI: 10.1016/j.cose.2004.05.002. ISSN 0167-4048.

[8] Recommendation X.509 | ISO/IEC 9594-8. The Directory: Public-Key and Attribute Certificate Frameworks. Open Systems Interconnection, 2008. 162+ s.

[9] Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0. OASIS Open, 2005.

[10] Radha, V., Reddy, D. H. A Survey on Single Sign-On Techniques. Procedia Technology. [Verkkolehti] Vol. 4, 2012. S. 134–139. [Viitattu 28.06.2012] DOI: 10.1016/j.protcy.2012.05.019. ISSN 2212-0173.

[11] Hardt, D. The OAuth 2.0 Authorization Framework. Internet Engineering Task Force, Reguest for Comments 6749, October, 2012.

[12] Cser, A et al. Forrester TechRadar™: Identity And Access Management Q2 2008. [Online]. Forrester Research Inc, 2008. [Viitattu 28.6.2012]. Saatavissa: http://www.forrester.com/Andras-Cser/research?N=10001+51762&range=504005&access=0&sort=2&source=hub#/Forrester+TechRadar+Identity+And+Access+Management+Q2+2008/quickscan/-/E-RES45768

[13] Bertino E. et al. Security For Web Services and Service-Oriented Architectures. Springer-Verlag Berlin Heidelberg, 2010. ISBN 9783540877417.

[14] SAML 101. [Online]. Ping Identity Corporation, 2012. [Viitattu 4.9.2012]. Saatavissa: https://www.pingidentity.com/unprotected/upload/SAML-101.pdf.

[16] Pankkien TUPAS-tunnistuspalvelupalveluntarjoajille. [Online]. Finanssialan keskusliitto, 2011. [Viitattu 27.7.2012]. Saatavissa: http://www.fkl.fi/teemasivut/sahkoinen_asiointi/Dokumentit/Tupas-varmennepalvelu_v23c.pdf.

[15] Vetuma-palvelu, Yleistä tietoa kansalaisen verkkotunnistamisen ja -maksamisen palvelusta. [Online]. Valtiokonttori, 2011. [Viitattu 5.9.2012]. Saatavissa: https://www.suomi.fi/suomifi/tyohuone/yhteiset_palvelut/verkkotunnistaminen_ja_maksaminen_vetuma/yleista_tietoa_vetumasta/Vetuma_palvelun_yleisesittely/Vetuma_palvelun_yleisesittely.pdf.

[17] Suomalaisen julkishallinnon Vetuma-palvelu, SAML-kutsurajapinnan määrittely. [Online] Valtiokonttori, 2012. [Viitattu 5.9.2012]. Saatavissa: http://www.suomi.fi/suomifi/tyohuone/yhteiset_palvelut/verkkotunnistaminen_ja_maksaminen_vetuma/tekninen_rajapinta/tekninen_rajapinta/03_vetuman_saml_kutsurajapinnan_maarittely_versio_1.1/vetuman_saml_kutsurajapinnan_maarittely_versio_1.0.pdf.

[18] OpenID Authentication 2.0 - Final. OpenID Foundation, 2007.

[19] T. Berners-Lee et al. Uniform Resource Identifier (URI): Generic Syntax. Internet Engineering Task Force, Request for Comments 3986, Januray, 2005.

[20] Extensible Resource Identifier (XRI) Syntax V2.0. OASIS Foundation, 2005.

[21] Miller, J. Yadis Specification, version 1.0. 2006. [Viitattu 20.8.2012] Saatavilla: http://archive.cweiske.de/yadis/yadis-v1.0.pdf.

[22] Fumy W., Sauerbrey J. Identity & Access Management Faster ROI and improved security through efficient assignment of rights and access control. The Practical Real-Time Enterprise. Springer Berlin Heidelberg, 2005. S 259–274. DOI: 10.1007/3-540-27367-0_16. ISBN 978-3-540-21995-8.

[23] Malville, E., Malville, C. & Gourmelen, G. A survey on identity federation solutions.. Annales Des Télécommunications. [Verkkolehti]. Vol 61:3–4, 2006. S 379-398. [Viitattu: 1.8.2012]. DOI: 10.1007/BF03219913.

[24] Pashalidis, A., Mitchell, C. A Taxonomy of Single Sign-On Systems. Information Security and Privacy. [Verkkolehti]. Vol. 2727, 2003. S 249–264. DOI: 10.1007/3-540-45067-X_22.

[25] Implementing Enterprise Single Sign-On in an Identity Management System. [Online]. Oracle, 2010. [Viitattu 15.9.2012]. Saatavilla: http://www.oracle.com/us/products/middleware/identity-management/wp-esso-idm-207215.pdf.

[26] Chong, F. Identity and Access Management. [Online]. Microsoft Corporation, 2004. [Viitattu 19.1.2013]. Saatavissa: http://msdn.microsoft.com/en-us/library/aa480030.aspx.

[27] Kerberos: The Network Authentication Protocol. [Online]. Massachusetts Institute of Technology, 2012 [Viitattu 19.1.2013]. Saatavissa: http://web.mit.edu/kerberos/.

[28] Microsoft.Active Directory Federation Services. [Online]. Microsoft Corporation. [Viitattu 19.1.2013]. Saatavissa: http://msdn.microsoft.com/en-us/library/bb897402.aspx.

[29] OASIS Service Provisioning Markup Language (SPML) Version 2. OASIS Open, 2006.

[30] Sodhi, G. User provisioning with SPML. Information Security Technical Report. [Verkkolehti]. Vol 9:1, 2004. S 86–96. DOI: 10.1016/S1363-4127(04)00018-4. ISSN 1363-4127.

[31] Spaulding, K., Bohren, J. Service Provisioning Mark-upLanguage (SPML) - Where we are, how we got here, and where we are going. [Online]. OASIS Open. [Viitattu 29.8.2012]. Saatavissa: http://xml.coverpages.org/Spaulding-Bohren-SPML-Past-Present-Future-Webinar.pdf.

[32] Harding, P. Why SCIM over SPML? Why not? [Online]. Ping Identity Corporation, 2011. [Viitattu 12.1.2013]. Saatavissa: https://www.pingidentity.com/blogs/pingtalk/index.cfm/2011/4/29/Why-SCIM-Why-not-SPML.

[33] Drake, T. et al. System for Cross-Domain Identity Management: Protocol. Internet Engineering Task Force, Internet Draft (work in progress), March, 2012.

[34] Fielding, R., T. Architectural Styles and the Design of Network-based Software Architectures. [Online]. Tohtorin väitöskirja. University of California, Department of Information and Computer Science. Irvine, USA, 2000. 180 s. [Viitattu 4.9.2012]. Saatavissa: http://www.ics.uci.edu/~fielding/pubs/dissertation/fielding_dissertation.pdf.

[35] SCIM / Overview. [Online]. Internet Engineering Task Force. [Viitattu 3.9.2012]. Saatavissa: http://www.simplecloud.info/#overview.

[36] Howes T., Smith M., Good, G. S. Understanding and Deploying Ldap Directory Services. 2nd ed. Addison-Wesley Professional, 2003. 899 s. (Network architecture and development series). ISBN 9780672323164 (painettu).

[37] What is Directory Service. [Online]. The Hong Kong University of Science and Technology. 16.8.2000. [Viitattu 22.8.2012]. Saatavissa: http://www.ust.hk/itsc/ldap/whatis.html.

[38] Sermersheim, J. Lightweight Directory Access Protocol (LDAP): The Protocol. Internet Engineering Task Force, Request for Comments 4511, June, 2006.

[39] Recommendation X.500 | ISO/IEC 9594-8. The Directory: Public-Key and Attribute Certificate Frameworks. Open Systems Interconnection, 2008. 162+ s.

[40] Carter, G. LDAP System Administration. O'Reilly Media, Inc., 2003. 294 s. (O'Reilly Series). ISBN 9781565924918 (painettu).

[41] eXtensible Access Control Markup Language (XACML) Version 2.0. OASIS Open, 2005. 141 s.

[42] Kasanen, H., Kangas, J. Vettä hanasta, identiteetinhallintaa töpselistä: Identiteetinhallinnan pilvipalvelut Suomessa. [Online]. Secproof Finland, 2010. [Viitattu 28.6.2012]. Saatavissa: http://www.secproof.com/media/Documents/Secproof_Identiteetinhallinnan_pilvipalvelut_Suomessa.pdf.

[43] Kasanen, H.Keskitetty identiteetinhallinta: Referenssiarkkitehtuuri. [Online]. Secproof Findand, 2010. [Viitattu 4.9.2012]. Saatavissa: http://www.secproof.com/media/Documents/Secproof_IdM_Referenssiarkkitehtuuri.pdf.

[44] Aharam, P. Identity Management PART II: User Provisioning Best Practices. [Online]. Aspen Advisors, 2011. [Viitattu 4.9.2012]. Saatavissa: http://aspenadvisors.net/sites/default/themes/asp/files/User_Provisioning_Best_Practices.pdf.

[45] Cser, A. The Forrester Wave™: Identity AndAccess Management Q4 2009. [Online]. Forrester Research Inc, 2009. [Viitattu 28.6.2012] Saatavissa: http://www.ca.com/us/~/media/files/industryanalystreports/iamforresterq4_2009_221389.aspx.

[46] Create a Free Online Survey. [Online] Freeonlinsurveys.com. [Viitattu 15.12.2012]. Saatavissa: http://freeonlinesurveys.com/.

[47] World's Largest Professional Network | Linkedin. [Online]. LinkedIn Corporation. [Viitattu 15.12.2012]. Saatavissa: http://www.linkedin.com/.

[48] Mauranen, K. Biostatiikka. [Online]. Kuopion Yliopisto, 1995. [Viitattu 28.12.2012]. Saatavissa: http://www.uku.fi/~mauranen/bis/bis6_doc.htm.

[49] Definition of cloud computing in Oxford Dictionaries. [Online]. Oxford Dictionaries. [Viitattu: 22.8.2012]. Saatavissa: http://oxforddictionaries.com/definition/english/cloud%20computing.

[50] Armbrust, M. et al. A View of Cloud Computing. Commun. ACM. [Verkkolehti]. Vol. 53:4, 2010. S. 50–58. [Viitattu 23.8.2012] DOI: 10.1145/1721654.1721672. ISSN 0001-0782.

[51] Mather, T. et al. Cloud Security and Privacy. O'Reilly Media, Inc., 2009. 338 s. (Theory in practice). ISBN 9781449379513 (painettu).

[52] Mell, P., Grance, T. The NIST Definition of Cloud Computing. [Online]. National Institute of Standards and Technology, 2011. [Viitattu 2.9.2012]. Saatavissa: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[53] Security Guidance for Critical Areas of Focus in Cloud Computing V2.1. [Online]. Cloud Security Alliance, 2009. [Viitattu 2.9.2012]. Saatavissa: https://cloudsecurityalliance.org/csaguide.pdf.

[54] The Intersection of Identity Management and Cloud Computing. [Online]. Hitachi ID Systems, Inc., 2011. [Viitattu 1.9.2012]. Saatavissa: http://hitachi-id.com/cgi-bin/emaildoc?document=intersection-of-identity-management-and-cloud-computing.pdf.

[55] Rong, C. et al. Beyond lightning: A survey on security challenges in cloud computing. Computers & Electrical Engineering. [Verkkolehti]. Vol 39:1, 2013. S. 47–54. DOI: 10.1016/j.compeleceng.2012.04.015. ISSN 0045-7906.

[56] Direktiivi 95/46/EY. Euroopan parlamentin ja neuvoston direktiivi 95/46/EY annettu 24 päivänä lokakuuta 1995, yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta. Euroopan parlamentti ja neuvosto. 1995. 24 s.

[57] Jaeger, P., T. et al. Identifying the security risks associated with governmental use of cloud computing. Government Information Quarterly. [Verkkolehti]. Vol. 27:3, 2010. S. 245–253. DOI: 10.1016/j.giq.2010.01.002. ISSN 0740-624X.

[58] Armbrust, M. et al Above the Clouds: A Berkeley View of Cloud Computing. [Online]. Electrical Engineering and Computer Sciences, University of California, 2009. [Viitattu 7.9.2012]. Saatavissa: http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf .

[59] Whitman, M. E., Mattor, H. J. Principles of Information Security. Course Technology Ptr, 2011. ISBN 9781111138219 (painettu).

[60] Kumaraswamy, S. et al. Domain 12: Guidance for Identity & Access Management V2.1. [Online]. Cloud Security Alliance, 2010. [Viitattu 8.2.2012]. Saatavissa: https://cloudsecurityalliance.org/guidance/csaguide-dom12-v2.10.pdf.

LIITE I: Asiantuntijakyselyn kyselylomake

Personal information

*Name

*Short description of professional background and experience in IAM systems:

*Company

Country

* What are the strengths of current IAM technology?

* What about the weaknesses?

* What do you think are the biggest threats to IAM in general?

* In general, across different vendors, how difficult would you rate the initial setup and system integration of complete IAM systems? (1 easy - 5 difficult)

- 1
- 2
- 3
- 4
- 5
- Not sure

* In a general, across different vendors, which parts or functionalities of IAM system products do you feel need improvement and how much? (1 not at all - 5 a lot)

	1	2	3	4	5	Not sure
Provisioning						
Federation						
Directory services						
Deprovisioning						

Authentication						
Authorization						
Monitoring						
Reporting						
Usability for end users						
Delegated administration and self-service						
Policy management						
Role management						
Segregation of duties						

Is there something else that you think needs improvement other than what was mentioned in the previous question?

Are there some features or functionalities that currently don't exist that you'd like to see in the future?

* How much do you believe the following trends will influence the IAM scene (1 not at all - 5 a lot)

	1	2	3	4	5	Not sure
Cloud services						
Mobile client devices (technical perspective)						
User-centricity						
Bring Your Own Device practices (policy and security perspective)						
Context-based identity management						

Are there some other trends that you think will influence IAM systems in the future?

* What do you think are the biggest barriers or threats to the previously mentioned trends?

* What do you think about IAM systems moving to cloud services in general?

Do you believe that moving to cloud services will ease or make harder IAM system

***1) implementation**

***2) usage**

***3) management**

* Do you believe the fundamentals of IAM systems will have to change in the future or are they well grounded?

Anything else to comment about IAM systems or IAM in general?